

AN INVESTIGATION OF DEVELOPMENTS IN WEB 3.0: OPPORTUNITIES, RISKS, SAFEGUARDS AND GOVERNANCE

By
Hendrik Jacobus Bruwer

*Thesis presented in partial fulfilment of the requirements for the degree Masters of Commerce
(Computer Auditing), at Stellenbosch University*



Supervisor: Mr. Riaan J. Rudman
Faculty of Economic and Management Science

"

*****Cr tkl4236

DECLARATION

By submitting this thesis/dissertation electronically, I declare that

- the entirety of the work contained therein is my own, original work,
- I am the sole author thereof (save to the extent explicitly otherwise stated),
- reproduction and publication thereof by Stellenbosch University will not infringe any third party rights, and
- I have not previously in its entirety or in part submitted it for obtaining any qualification.

December 2013

Copyright © 2016 Stellenbosch University.

All rights reserved.

ABSTRACT

Many organisations consider technology as a significant asset to generate income and control cost. The World Wide Web (henceforth referred to as the Web), is recognised as the fastest growing publication medium of all time, now containing well over 1 trillion URLs. In order to stay competitive it is crucial to stay up to date with technological trends that create new opportunities for organisations, as well as creating risks. The Web acts as an enabler for technological advancement, and matures in its own unique way. From the static informative characteristics of Web 1.0, it progressed into the interactive experience Web 2.0 provides. The next phase of Web evolution, Web 3.0, is already in progress.

Web 3.0 entails an integrated Web experience where the machine will be able to understand and catalogue data in a manner similar to humans. This will facilitate a world wide data warehouse where any format of data can be shared and understood by any device over any network. The evolution of the Web will bring forth new opportunities as well as challenges. Organisations need to be ready, and acquire knowledge about the opportunities and risks arising from Web 3.0 technologies.

The purpose of this study is to define Web 3.0, and identify new opportunities and risks associated with Web 3.0 technologies by using a control framework. Identified opportunities can mainly be characterised as the autonomous integration of data and services which increases the pre-existing capabilities of Web services, as well as the creation of new functionalities. The identified risks mainly concern unauthorised access and manipulation of data; autonomous initiation of actions, and the development of scripts and languages. Risks will be mitigated by control procedures which organisations need to implement (examples include but is not limited to encryptions; access control; filtering; language and ontology development control procedures; education of consumers and usage policies). The findings will assist management in addressing the key focus areas of opportunities and risks when implementing a new technology.

UITTREKSEL

Baie organisasies beskou tegnologie as 'n belangrike bate om inkomste te genereer en kostes te beheer. Die Wêreldwye Web (voorts na verwys as die Web), word erken as die vinnigste groeiende publikasiedmedium van alle tye, met tans meer as 1 triljoen URLs. Ten einde kompetender te bly, is dit noodsaaklik om op datum te bly met tegnologiese tendense wat nuwe geleenthede, sowel as risikos, vir organisasies kan skep. Die Web fasiliteer tegnologiese vooruitgang, en ontwikkel op sy eie unieke manier. Vanaf die statiese informatiewe eienskappe van Web 1.0, het dit ontwikkel tot die interaktiewe ervaring wat Web 2.0 bied. Die volgende fase van Web-ontwikkeling, Web 3.0, is reeds in die proses van ontwikkeling.

Web 3.0 behels 'n geïntegreerde Web-ervaring waar 'n masjien in staat sal wees om data te verstaan en te kategoriseer op 'n soortgelyke wyse as wat 'n mens sou kon. Dit sal lei tot 'n wêreldwye databasis waar enige vorm van data gedeel en verstaan kan word deur enige toestel oor enige netwerk. Die ontwikkeling van die Web sal lei tot die ontstaan van nuwe geleenthede, sowel as uitdagings. Dit is noodsaaklik dat organisasies bewus sal wees hiervan, en dat hulle oor genoegsame kennis sal beskik met betrekking tot die geleenthede en risikos wat voortspruit uit Web 3.0 tegnologieë.

Die doel van hierdie studie is om Web 3.0 te definieer, en nuwe geleenthede en risikos wat verband hou met Web 3.0 tegnologieë, te identifiseer deur gebruik te maak van 'n kontrole raamwerk. Geleenthede wat geïdentifiseer is, word hoofsaaklik gekenmerk deur outonome integrasie van data en dienste wat lei tot 'n toename in die vermoëns van reeds bestaande Webdienste, sowel as die skepping van nuwe funksionaliteite. Die risikos wat geïdentifiseer is, word hoofsaaklik gekenmerk deur ongemagtigde toegang en manipulasie van data; outonome inisieering van aksies, en die ontwikkeling van programskrifte en tale. Risikos wat geïdentifiseer is, sal aangespreek word deur die implementering van voorgestelde kontroleprosedures om sodanige risikos te verminder tot 'n aanvaarbare vlak (voorbeeld sluit in maar is nie beperk tot enkripsie; toegangskontroles; filters; programmatuur taal en ontologie ontwikkel kontroles prosedures; opleiding van gebruikers en ontwikkelaars en beleide ten op sigte van gebruik van tegnologieë). Die bevindinge sal bestuur in staat stel om die sleutelfokus-areas van geleenthede en risikos te adresseer gedurende die implementering van 'n nuwe tegnologie.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION, RESEARCH OBJECTIVE AND METHODOLOGY	9
1.1 Introduction	9
1.2 Research Objective.....	9
1.3 Research Motivation	10
1.4 Scope Limitations.....	10
1.5 Methodology	10
 CHAPTER 2: LITERATURE REVIEW	 14
2.1 Introduction	14
2.2 Historic review	14
2.3 Definition	15
2.3.1 Web 1.0.....	15
2.3.2 Web 2.0.....	16
2.3.3 Web 3.0.....	19
2.4 Corporate governance	22
2.5 IT governance.....	23
2.5.1 The advantages of implementing IT governance principles.....	24
2.5.2 Risks of non-compliance with IT governance principles	24
2.6 Control framework	24
2.6.1 COBIT defined	24
2.6.2 Advantages of implementing COBIT	26
2.6.3 Disadvantages of implementing COBIT	26
2.7 Business assumptions and business imperatives	Error! Bookmark not defined.
2.7.1 Basic business assumptions	Error! Bookmark not defined.
2.7.2 Business imperatives	Error! Bookmark not defined.
2.8 Conclusion.....	26
 CHAPTER 3: FINDINGS	 27
3.1 Introduction	27

3.2 Defining technologies associated with Web 3.0	27
3.2.1 Extensible Markup Language	28
3.2.2 Simple Object Access Protocol	28
3.2.3 Resource Description Framework	28
3.2.4 Resource Description Framework Schema.....	29
3.2.5 Structured Query Language and Simple protocol and RDF query Language	29
3.2.6 Ontology Web Language and Web Ontology Language for Services	29
3.2.7 Intelligent agents.....	30
3.2.8 Conclusion.....	31
3.3 Opportunities or possible uses for Web 3.0	32
3.3.1 Introduction	32
3.3.2 Web-services	32
3.3.3 Agent-based information harvesting and distribution	33
3.3.4 Search engine capabilities	34
3.3.5 Business intelligence	35
3.3.6 Knowledge management	37
3.3.7 eLearning and research.....	38
3.3.8 Inbound marketing.....	40
3.3.9 Conclusion.....	41
3.4 Risks associated with Web 3.0.....	41
3.4.1 Introduction	41
3.4.2 Unauthorised access to sensitive information	42
3.4.3 Hyper-targeted spam.....	43
3.4.4 Identity theft and social phishing.....	44
3.4.5 Autonomous initiation of instructions and malicious script injections	45
3.4.6 Development of ontologies.....	46
3.4.7 Proof and trust standardisation	46
3.4.8 Internationalisation – multilingualism.....	47
3.4.9 Conclusion.....	48

3.5 Safeguards and controls to mitigate risks.....	48
3.5.1 Introduction	48
3.5.2 Controls	48
3.5.3 Conclusion.....	53
CHAPTER 4: CONCLUSION	53
REFERENCES	60

LIST OF FIGURES, TABLES AND APPENDICES

Figures:

Figure 1: A comparison between Web 1.0 and Web 2.0 technologies.....19

Figure 2: The technological layout of Web 3.0.....29

Tables:

Table 1: Risks and safeguards associated with Web 3.0 technologies identified.....61

Appendices:

Appendix 1: Control framework COBIT 5 control processes identified which can be implemented to mitigate risks associated with Web 3.0 technologies.....78

CHAPTER 1: INTRODUCTION, RESEARCH OBJECTIVE AND METHODOLOGY

1.1 Introduction

Many organisations define technology as a significant asset to generate income and control cost (Brynjolfsson & Hitt, 2000). The World Wide Web (henceforth referred to as the Web), is recognised as the fastest growing publication medium of all time, containing well over 1 trillion URLs (Alpert & Hajaj, 2008). With an estimated growth rate of 566% in Internet usage in the last twelve years (Internet World Stats, 2012), the Internet has become the main source of communication worldwide. With ever increasing growth rates, the technology supporting the structure of the Internet is evolving at an even higher rate. Keeping abreast with technological trends creates new opportunities for organisations (International Data Corporation, 2012).

The Web, acting as an enabler for technological advancement, matures in its own respective way. Initially there were the static informative characteristics of Web 1.0 which progressed into the passive and interactive experience of Web 2.0. The next phase of Web evolution, Web 3.0, is already in progress.

The evolution of the Web will bring forth new opportunities, as well as challenges. Web 3.0 will change the way people interact with devices and networks, and how companies use information to market and sell their products, and operate their businesses (Booz & Company, 2011). Organisations need to be ready and acquire knowledge about the opportunities and risks arising from Web 3.0 technologies.

1.2 Research Objective

The objective of this study is to investigate the impact of Web 3.0, and its applications on business operations. The study aims to identify and define opportunities and risks arising from Web 3.0 technologies within different areas of operations. By implementing the relevant control processes of a best practised IT control framework, these risk areas will be minimised.

The study proposes to provide knowledge to organisational leaders, managers, boards of directors, IT professionals and information managers with regard to opportunities and risks

arising from the use of Web 3.0 and its applications, and to recommend possible safeguards to mitigate these risks to an acceptable level.

1.3 Research Motivation

Web 3.0 calls for a complete reconstruction of Internet and IT infrastructure. Organisations need to start preparing for the changes accompanying this technology before the third version of the Web is fully realised, otherwise they may be unable to satisfy customer needs, capitalise on emerging trends, and seize new opportunities (Spencer, 2009). Before these changes in infrastructure are adopted, organisations need to fully understand the impact the technology will have on business operations.

Defining opportunities of Web 3.0 is complicated, and needs to be investigated on an operational level to understand what impact the technology will have on business drivers. On the whole, organisations believe that new technology brings positive opportunities to their businesses, while a small percentage sees technology trends as having a negative impact (The Economist Intelligent Unit, 2013). Organisations need to be made aware of the risks associated with the use of Web 3.0 and its accompanying applications, and need to implement methods to mitigating these risks to an acceptable level.

1.4 Scope Limitations

Business drivers for each organisation vary, and are specific to the industry in which the organisation operates. The purpose of the study is to investigate the impact Web 3.0 technologies will have on broad based business drivers which are applicable to most industries and companies. The focus will not be on industry-specific business drivers.

The focus of the research is on incremental risks specifically pertaining to Web 3.0, and not all the risks prevalent to Web 2.0, or other pre-existing internet risks. The purpose is not to discuss the underlying technologies of Web 3.0 in detail, but rather to highlight the risks arising from the use of these technologies. Some of the prevalent risks associated with previous Web generations will be reinvestigated since the underlying technology creating these risks, has changed.

1.5 Methodology

A non-empirical study reviewing papers published in accredited research journals, articles and whitepapers in publications and Websites, will be conducted. In order to accumulate

knowledge Webster and Watson (2002) argued that an effective review of historic and applicable literature needs to be performed. They criticised the Information System (IS) field for the lack of theoretical outlets due to the complex nature of assembling a literature review on interdisciplinary fields.

In order to add scientific rigour to a literature review, a four stage approach is suggested by Sylvester, Tate and Johnstone (2011). This four stage approach was followed by the researcher, and each stage was repeated and performed interactively. A wide selection of articles and readings were selected at the beginning stages to enable a comprehensive understanding of the underlying literature, and the selection was narrowed down to more specific areas at the latter stages. The literature was selected within a timeline between 1996 and 2013.

The following stages as suggested by Sylvester *et al.* (2011) were carried out by the researcher:

1. The searching stage: The initial search terms were intentionally selected to include a broader spectrum of results, and included, *inter alia*, 'Web 3.0'; 'semantic Web'; 'next generation Web service'; 'Technologies driving Web 3.0'; 'impact of Web 3.0 on business processes'; 'control framework for IT governance', and 'defining Web 3.0 technologies'. The search was enabled through the use of library books and different electronic databases like professional subscriptions; scholar articles (Google scholar), organisational whitepapers and electronic journals (such as *IEEE*, *Gartner*, *Google Scholar*, *Elsevier*, *Emerald*). Due to the fact that minimum research has been completed on the subject, the reputational value of the articles was originally not taken into account during the selection. The search yielded a set of 140 articles and Website entries.

2. The mapping stage: During this stage the original selection was narrowed down by selecting articles and readings that had a similar running theme. The similarities in the selection included the following recurring themes, *inter alia*, 'Web 3.0 and businesses'; 'risks associated with Web 3.0 and semantic Web'; 'opportunities and Web 3.0'; 'impact of new technologies on business', 'technologies supporting Web 3.0/semantic Web'; 'COBIT control framework', and 'Web 3.0 and semantic Web control'. This enabled the researcher to narrow down the original selection by reviewing extracts and summaries of the articles and readings. The original selection was reduced to 75 items.

3. The appraisal stage: An in depth reading of the narrowed down selection enabled the researcher to develop a concept of Web 3.0 and underlying technologies, and to elaborate on

the impact these technologies will have on business operations. The different concepts were annotated within the articles.

4. The synthesis stage: During this stage the researcher compiled all annotations and generated his own conclusions through integrating, modifying and generalising the main concepts found in the previous three stages into a single flowing document.

The stages described above enabled the researcher to acquire a better understanding and to elaborate on the following topics:

- Definition of Web 3.0
- Impact of Web 3.0 on business operations
- New business opportunities and risks accompanying Web 3.0
- Control frameworks

In order to address the research problem the research will be structured using the following steps:

- Step 1: **Define Web 3.0.** A formal definition is needed to categorise the new technologies within Web 3.0. Definitions available for Web 3.0 are arbitrary at best since minimal research has been performed on the subject. The purpose is to create a rational definition compiled from research and available literature.
- Step 2: **Identify the impact Web 3.0 technologies will have on existing business operations.** Web 3.0 will redefine existing business operations, or subjectively create new Web 3.0 specific business operations.
- Step 3: **Report on the effect the impact Web 3.0 technologies will have on business operations.** The influence on business operations will give rise to new opportunities and strategic risks associated with the effects of Web 3.0 technologies.
- Step 4: **Identify the risks associated with the changes in business operations** due to the impact of Web 3.0 technologies, and how they correlate.
- Step 5: **Perform a detailed study of COBIT control framework, and use the framework to identify risks associated with Web 3.0.** After identifying the

risks framework controls will be mapped to the relevant risks that will mitigate the risks to an acceptable level.

By implementing the methodology, a more detailed understanding of Web 3.0 and the underlying technologies, risks and controls associated with Web 3.0, can be obtained.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

Web 3.0 is the latest evolution in Internet communication, and will not only restructure Internet communication, but will also have a significant impact on crucial business drivers. Web 3.0 will not only give rise to new business drivers, but will also redefine existing drivers.

The exact interpretation of what Web 3.0 technologies will ultimately entail and how it will influence the Web experience, is not hundred percent clear, but an array of opportunities arise for innovative services, methods and applications with the introduction of these technologies (Knublauch, Ferguson, Noy & Musen, 2004). Missing opportunities are not the only area of concern for organisations when analysing the risks promoted by these new technologies.

2.2 Historic review

Historical research on the evolution of the Web shows patterns and goes through similar phases. Initial research focused on defining the technology, understanding its benefits, and how it will have an impact on business environments regarding opportunities and challenges (Clearswift, 2007, O'Reilly, 2009). Research inquiring about user behaviour and privacy issues (Lawler & Molluzzo, 2010), focusing on knowledge of personal information gathering, and sharing techniques on Web technologies, has also been undertaken. As the Web evolved and the technologies surrounding it became more popular, the focus shifted to security risks, especially focusing on business risks (Grossman, 2007; Websense, 2009).

The latest research into Web evolution conducted by Benjamins, Contreras, Oscar, Corcho and Gómez-Pérez (2002), focuses on defining and predicting the challenges arising from the use of Web 3.0 technologies. Related research by Lu, Dung and Fotouhi (2002) investigates possible opportunities and complications Web 3.0 might offer, and how an enterprise can gain business value from using these applications.

The extent to which technology has been incorporated into business activities has created a critical dependency on Information Technology (IT) that calls for a specific focus on IT governance (van Grembergen & De Haes, 2008). Various attempts have been made to develop an organisational framework to help businesses to mitigate the risk arising from the use of Web technology (Rudman, 2010). Dawson (2007, 2008) tried to develop a widely used

framework in an effort to help businesses not just to understand and mitigate risks, but also to add business value from using Web technologies. A further study by Rudman (2010) specifically considers the incremental risk arising from Web 2.0 technologies, and the creation of a comprehensive control framework to mitigate the risk of unauthorised access.

The majority of research completed on Web 3.0 was performed by independent private organisations like Booze & Company; Verizon; Gartner, Clearswift and SEM Logic. Most of the research consists of whitepapers and articles with very little academic peer-reviewed articles. Most of the articles aim to define Web 3.0, and rarely address advantages and disadvantages arising from use of Web 3.0 technologies. A study that focuses on defining Web 3.0, identifying the business risks and opportunities arising from the use of this technology, and the creation of a comprehensive control framework to mitigate these risks, has not been conducted.

To understand in what direction the Web is heading and what impact it will have on organisations, it helps to define the various stages of the Web. Since minimal research has been conducted on Web 3.0 or the impact Web 3.0 will have on business and business operations, defining Web 3.0 will be the starting point.

2.3 Definition

Web 3.0 is a new concept in the domain of Web evolution. The definition will assist in categorising the new and developing Web technologies into the correct evolutionary genre. It will also assist in distinguishing between pre-existing and new risks and opportunities arising from Web 3.0 technologies. In order to define Web 3.0 its predecessors, Web 1.0 and Web 2.0, need to be evaluated in order to obtain a full comprehension of how Web 3.0 evolved.

2.3.1 Web 1.0

According to O'Reilly (2007), during the first Web 2.0 Conference, in October 2004, it was hard to list a preliminary set of principles by which the difference between Web 1.0 and Web 2.0 could be distinguished.

Web 1.0 was a platform through which information could be published in a static form well designed with text and images (DCruz, 2009). It portrayed an environment where information and data were static, and displayed with no interaction between the

information and the consumer, and minimal content creators, also known as the read-only Web.

The protocols associated with this generation were Hypertext Transfer Protocol (HTTP) and Hypertext Markup Language (HTML). The HTTP protocol transfers information between a Web server and a Web browser. HTML protocol communicates with the browser, and informs it how to display whatever text, graphics and images transferred by the HTTP protocol (Berners-Lee, 1996). Viewing the data displayed was the only interaction the consumer had with the content. The consumer was not able to create or add new content which defines Web 1.0.

2.3.2 Web 2.0

O'Reilly Media and Media Live International (2007) first introduced the term Web 2.0 in October 2004. When the inventor of the Web, Sir Tim Berners-Lee, was asked in a podcast what the difference was between Web 1.0 and Web 2.0, he replied as follows (developerWorks Interviews, 2006):

"Web 1.0 was all about connecting people. It was an interactive space, and I think Web 2.0 is of course a piece of jargon, nobody even knows what it means. If Web 2.0 for you is blogs and wikis, then that is people to people. But that was what the Web was supposed to be all along. And in fact, you know, this 'Web 2.0', it means using the standards which have been produced by all these people working on Web 1.0."

The main consensus was that Web 2.0 is not a new development of the Web, but rather an extension of the original ideals and principles of Web 1.0, and does not warrant a special moniker (Anderson, 2007).

In an effort to clarify the paradigm shift Cormode and Krishnamurthy (2008) stated that the main difference between Web 1.0 and Web 2.0 is not the underlying infrastructure of the Web, but rather the ability of consumers to create content on the Web. With the evolution of the Web, new technological aids made it possible for consumers to create content on the Web and share it. Getting (2007) describes it as the greater collaboration between consumers, programmers, service providers and organisations, which enables them to re-use and contribute information, and thereby enriching the content distributed between the collaborative parties on the Web.

Rudman (2010) categorises different classification methods in terms of components or features, technology and programming. Furthermore he summarises the key features of Web 2.0 sites into three components:

- **Community and social:** The ability of a consumer to view, create, edit and share content by means of the Web. This permits users to study, change and improve content or software (or source-code), and to simultaneously redistribute and re-use it in modified form. This includes the ability to post content in many forms: photos; videos; blogs, comments and ratings on other users' content; tagging of own or someone else's content, and some ability to control privacy and sharing (Cormode & Krishnamurthy, 2008).
- **Technology and architecture:** Software and applications with multiple device and platform compatibility. Software with the ability to deliver rich interfaces operable on any device or platform without the need of additional software installation.
- **Business and process:** Cloud technologies, software and resources made available on a network. The software is available on multiple platforms and devices, and is delivered as a service rather than an installed product. More technical features include a public Application Programming Interface (API) to allow third party enhancements and "mash-ups", and the ability to communicate with other users and colleagues through internal email or Instant Message (IM) systems (Cormode & Krishnamurthy, 2008).

A key feature identified and present in the research that has been reviewed, is that Web 2.0 is able to facilitate a more socially connected Web where everyone is able to add, edit, view and redistribute the information space (Anderson, 2007). Web 2.0's applications have the ability to harness collective intelligence, and in doing so combine and integrate Web content and services to improve the end user's experience (Giannakos & Lapatas, 2010).

Web 2.0 is an extension of Web 1.0 which still operates on the same ideals, principles and protocols, with extended collaboration between consumers, and the ability to harvest and add content by consumers in an intelligent way to enable an enriched experience for the consumer.

Comparing the examples listed in Figure 1 will assist in formulating a sense of the technologies associated with Web 1.0 and Web2.0:

Figure 1: A comparison between Web 1.0 and Web 2.0 technologies:

Web 1.0	Web 2.0
DoubleClick	Google AdSense
Ofoto	Flickr
Akamai	BitTorrent
Mp3.com	Napster
Britannica Online	Wikipedia
Personal Websites	Blogging
Evite	Upcoming.org and EVDB
Domain name speculation	Search engine optimization
Page views	Cost per click
Screen scraping	Web services
Publishing	Participation
Content management systems	Wikis
Directories (taxonomy)	Tagging ("folksonomy")
Stickiness	Syndication

2.3.3 Web 3.0

The next generation of the Web, Web 3.0, is not represented by the emergence of a new Web but rather an extension and calibration of the technologies already present in Web 2.0. Internet content is becoming more diverse, and the volume of data is getting much larger, which makes management of information more critical (Bergman, 2001). The Web is becoming a platform for linked data. Data is becoming more openly available to consumers, and by making connection between similar data characteristics, the data itself becomes more valuable (Tarrant, Hitchcock & Carr, 2011). The Web is overrun with exabytes of data, and computers still cannot automate the function of harvesting this information, or of performing complex tasks with it (Intervise, n.d.). The need for data structuring and integration is crucial to enable the Web to evolve into its next phase.

Even though Web 3.0 will be the next generation of the Web, its definition varies (Farah, 2012). A variation in names is also apparent, and names include, amongst others: Web 3.0; The Semantic Web; The Transcendent Web and The Web of Things (henceforth referred to as Web 3.0). Even though the names differ, research shows that all these phrases have the same basic fundamentals.

In order to obtain a better understanding of what Web 3.0 consists of and how it functions, one needs to be familiar with specific terminology associated with Web 3.0 technologies. These terms are briefly discussed below in order to obtain sufficient knowledge to compile a definition of Web 3.0, but will be discussed in detail in chapter 4. The terms are categorised into 3 subsections, namely, identifiers, languages and structures, in order to illustrate how these technologies interact with each other to form the Web:

Section 1: Identifiers

- **Uniform Resource Identifiers (URI)** identifies the name and location of a file or resource in a uniform format. URI's provides a standard way for resources to be accessed by other computers across a network or over the Web (Tech Terms, 2013).
- **Uniform Resource Locator (URL)** is the address of a specific Website or file on the Internet (TechTerms, 2013).

Section 2: Structures

- **Metadata** is a term used to describe data within data. It provides information about a certain item's content (TechTerms, 2013).
- **Resource Description Framework (RDF)** is a specification that defines how metadata, or descriptive information, should be formatted. The RDF model uses a subject-predicate-object format, which is a standardised way of describing something (TechTerms, 2013).
- **Resource Description Framework Schema (RDFS)** is a set of classes with certain properties using the RDF extensible knowledge representation language, providing basic elements for the description of ontologies, otherwise called RDF vocabularies, intended to structure RDF resources (Wikipedia, 2013b).
- **Intelligent agents** are software programs designed to collect information based on the users' interaction with the Web. They can also act on behalf of the user to perform certain tasks and duties depending on the authorisation level granted to the intelligent agent by the user.

Section 3: Languages

- **Extensible Mark-up Language (XML)** is used to define documents with a standard format that can be read by any XML compatible application. The language can be used with HTML pages, but XML itself is not a mark-up language. Instead, it is a "meta-language" that can be used to create mark-up languages for specific applications.
- **SPARQL** is an RDF query language, that is, a query language for databases, able to retrieve and manipulate data stored in RDF format (Wikipedia, 2013c).
- **The Ontology Web Language (OWL)** is a set of mark-up languages which are designed for use by applications that need to process the content of information, instead of just presenting information to humans. OWL ontologies describe the hierarchical organisation of ideas in a domain, in a way that can be parsed and understood by software. OWL has more facilities for expressing meaning and semantics than XML, RDF and RDFS, and thus

OWL goes beyond these languages in its ability to represent machine interpretive content on the Web (Webopedia, 2013).

Wolfram (2010) stated that Web 3.0 is where the computer, rather than humans, is generating new information. This is supported by Morris' (2011) theory that integration of data is the basic foundation of Web 3.0, and by using metadata imbedded in Websites, data can be converted into useful information, and be located, evaluated, stored or delivered by intelligent agents. In order for intelligent agents to understand the information gathered, expressive languages that describe information in forms understandable by machines, need to be developed (Lu *et al.*, 2002).

With the development of expressive languages Web 3.0 has the capability to use unstructured information on the Web more intelligently by formulating meaning from the context in which the information is published (Verizone, n.d.). There is a need for Web 3.0 to express information in a precise, machine interpretive form, so that intelligent agents can process this data and not just share it, but understand what the terms describing the data mean (Noy, Sintek, Decker, Crubézy, Ferguson & Musen, 2001).

Booze & Company (2011) stated that recommendation engines will focus on habits and preferences of users, and in doing so will produce more complete and targeted information. The information of habits and preferences used on a recommendation engine will be collected and stored in a hierarchical manner by intelligent agents. This is what will give Web 3.0 the ability to gather, analyse and distribute data which can be turned into information, knowledge, and, ultimately, wisdom (Evans, 2011).

The key elements of Web 3.0 present in all the observations are (Verizon, n.d.):

- The **introduction of new programming languages** with the ability to categorise and manipulate data in order to enable machines to understand data, and the phrases describing data.
- The capability of **obtaining contextual information** from a Web search and storing it in a hierarchical manner, according to similar characteristics for easy and specific retrieval.
- The ability to obtain information from a **bigger and wider variety of sources**, including previously walled application.

- The **ability to create and share all types of data** over all types of networks by all types of devices and machines.

Web 3.0 will ultimately entail an integrated Web experience where the machine will be able to understand and catalogue data in a manner similar to a human. The data collected will be categorised in a hierarchical manner in order to link data with similar characteristics, and retrieve consumer specific data effectively and efficiently. This will facilitate a worldwide data warehouse where any format of data can be shared and understood by any device over any network.

With the adoption of new technologies, organisations are confronted with the new risks associated with these technologies. To lower the risk of exposure to these threats, organisations need to implement some form of corporate governance to guide management as well as employees to act in accordance with internationally acceptable standards and principles.

2.4 Corporate governance

Corporate governance can be viewed as the overall business structure and ethical values that supports the company in achieving its objectives, and which involves all parties, including the board of directors, senior management, shareholders, employees and any other related parties (Goosen, 2012). Thomson (2009) stated that corporate governance consists of governing mechanisms within an organisation. These mechanisms provide guidance to an organisation in order to fulfil its goals and reach its objectives in such a manner that value is added to the company and all related parties. It also forces the board of directors to act in the best interest of the company (PricewaterhouseCoopers, 2009).

With the ever increasing reliance on IT and emphasis placed on information by legislation, such as the Protection of Personal Information Bill; Protection of Information Bill, Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) and codes such as The King Report on Corporate Governance III, the responsibilities of managing and controlling IT risks and the information organisations possess, have become a vital part of corporate governance (South Africa, 2009). The process of managing IT has become more than mere technical functions carried out by IT experts, and now forms part of the essential management function within an organisation (Stoneburner, Goguen & Feringa, 2002).

In order to comply with regulatory governance, organisations must implement an effective IT governance policy to control the risks associated with the adoption of new Web 3.0 technologies.

2.5 IT governance

With the rapid change in IT it has become imperative for organisations to use IT effectively. Organisations need to implement an effective and adaptive IT governance policy to control the new risks arising from the adoption of new technologies like Web 3.0 (The National Computing Centre, 2005).

Weill (2004) describes IT governance as a set of principles that allocates accountability, and supports responsible parties in behaving in an acceptable way when it comes to decision making and the use of IT. He further elaborates by stating that IT governance is not about specific decision making, but rather about determining who makes what decisions, and how the decision makers are held accountable for their input. The King III report contains the corporate governance principles for South African organisations. The governance principles reported in King III led to the introduction of IT governance in South Africa, and form part of corporate governance principles that organisations in South Africa should apply (PricewaterhouseCoopers, 2009).

With business environments becoming more technologically advanced, and more reliance being placed on IT, the impact it has on business is not just operational, but strategic as well (Goosen, 2012). IT consists of all components of processing including the human, financial, physical and informational aspects of IT (Doughty & Grieco, 2004). IT is therefore not just an enabler on an operational level, but an asset which can assist in creating opportunities, and thereby ensure that an organisation gains a competitive advantage, and should be governed as such (PricewaterhouseCoopers, 2013). IT governance should support and broaden the board's mission of defining strategic direction, which includes implementing effective risk management systems and internal controls (Goosen, 2012); managing the responsible use of resources, and ensuring that overall organisational objectives are met (Gertz, Guldentops & Strous 2002). These objectives are commonly referred to as "strategic level" objectives.

The only way to create an environment where IT supports business goals; investment in IT yield a desirable return, and IT-related risks and opportunities are managed appropriately, is

by implementing sound IT governance practices which are reviewed and adapted to support the implementation of new technologies (IT Governance Institute, 2005). Organisations should seek assistance in implementing such policies by adopting an internationally approved framework.

2.5.1 The advantages of implementing IT governance principles

Implementing IT governance practices will lead to the following advantages:

- Strategic alignment between IT and business goals that will create a competitive advantage.
- Increased risk management procedures and a better understanding of IT, which will improve the decision making process.
- Greater compliance with governance requirements, laws and regulations.

2.5.2 Risks of non-compliance with IT governance principles

If IT governance principles are not implemented, it could give rise to:

- Operational risks, and threaten confidentiality, reliability and authenticity of data.
- Unauthorised access and changes to the IT system could occur, which impair the availability and functionality of the system.

2.6 Control framework

In order to ensure effective IT governance, organisations should make use of already established and internationally accepted frameworks as guidance. The Control Objectives for Information and related Technology (COBIT) provides a detailed framework, and describes the controls which need to be implemented in order to have a sound IT governance structure.

2.6.1 COBIT defined

COBIT is a detailed method to implement IT governance, and is internationally accepted as the best practical framework to assist in implementing IT governance to ensure sound IT controls (Hardy, 2006). COBIT consists of a framework that must be adjusted and used in collaboration with other resources in order to customise it, and make the guidelines applicable to an organisation's specific environment (Campbell, 2005). The purpose of COBIT framework is to guide management with controlling and managing information and

related technology. The framework describes the importance of IT resources (people, applications, technology, facilities and data), and how the information, with the assistance of IT processes, created by the resources, should be delivered in order for it to fully support the business objectives (Hussain & Siddiqui, 2005). This delivery is controlled through 37 high-level control objectives, one for each process, contained in five domains. Each domain is defined, and the processes within each specific domain are described. After the process has been defined and evaluated, the risks applicable to the specific process are identified. In order for the risks identified to be mitigated, the impact of the risk on the process is categorised as high, medium or low, and control objectives linked to this process. Each control objective can be used to create an activity or task in order to address the risks identified (Rudman, 2008). The five domains are described as follows:

- **Build, Acquire and Implement:** This domain covers identifying, developing and acquiring an IT solution that continues to support the business objectives. It also assists in creating IT maintenance policies to control changes and maintenance of the system in order to prolong the life of the IT system and its components (Sahibudin, Sharifi & Masarat, 2008; IT Governance Institute, 2005).
- **Monitor, Evaluate and Assess:** This domain entails the evaluation and validation of business and IT processing goals. It ensures that all IT processes are monitored regularly and in a timely manner, and that the monitored results are measured against the expected outcomes, and that any fluctuations are investigated (ISACA, 2012).
- **Delivery, Service and Support:** This domain covers the actual delivery of required services, including service delivery; management of security and continuity, and training and technical support for users (IT Governance Institute, 2005).
- **Align, Plan and Organise:** This domain covers strategy and tactics, and concerns the identification and implementation of a proper IT infrastructure that optimally utilises IT resources in order to best contribute to the achievement of the business objectives (IT Governance Institute, 2005).
- **Evaluate, Direct and Monitor:** All IT processes need to be regularly assessed over time in order to assess the effectiveness of the processes' ability to meet the business objectives. This includes assessing performance management and monitoring of internal control, regulatory compliance and governance (Sahibudin *et al.*, 2008; IT Governance Institute, 2005).

Each of these five domains will assist an organisation in implementing the controls needed to mitigate the risks identified and associated with the adoption of new Web 3.0 technologies.

2.6.2 Advantages of implementing COBIT

The following advantages were summarised by Rudman (2008), ITGI (2007) and Campbell (2005):

- Low implementation cost, and openly and electronically available.
- Created and applied by acclaimed international organisations, and covers a wide range of IT processes which ensures easy alignment with other international frameworks and standards.
- Ensures sound controls and regulatory compliance.

2.6.3 Disadvantages of implementing COBIT

Rudman (2008) underlined the following disadvantages organisations should take into account before implementing COBIT:

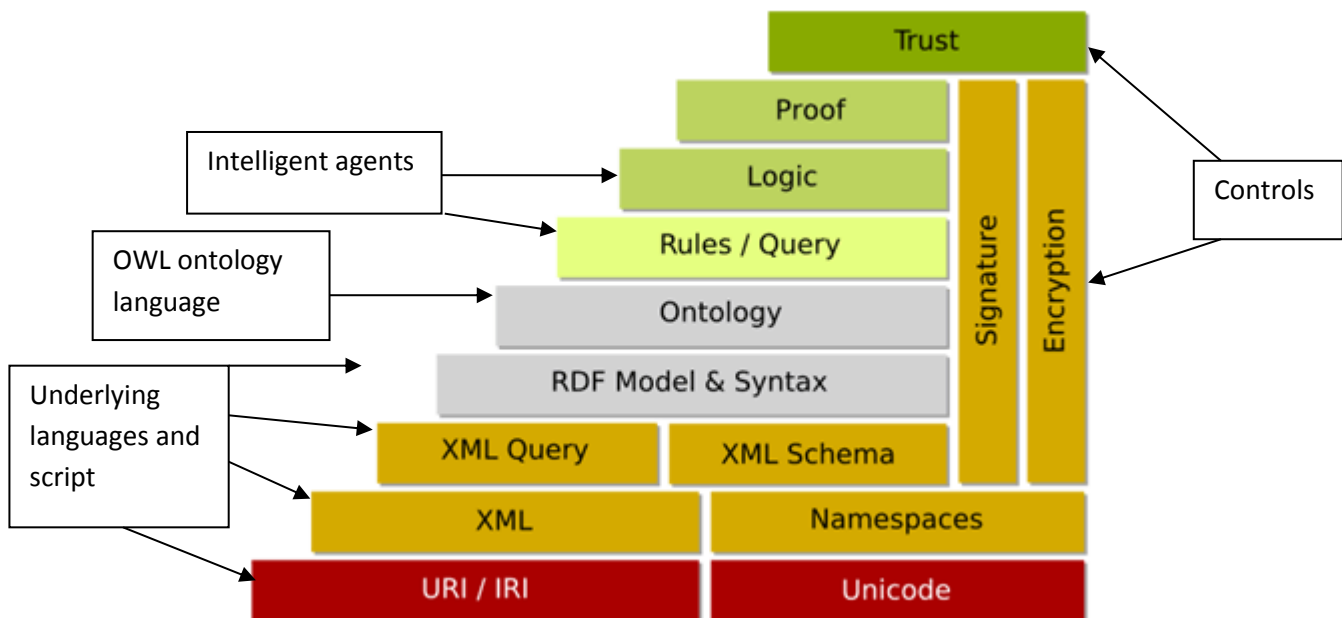
- There is a lack of detail on how the control processes should be implemented.
- COBIT has a wide range of IT processes and controls which create a lot of criteria. The level of detail can create compliance difficulties.
- COBIT does not elaborate enough on security issues.

2.8 Conclusion

After reviewing the literature above, the insight gained will be used to attempt to identify new advantages and risks that might arise from the use of Web 3.0 technologies. The risks will be mitigated by applying the applicable control objectives in a manner that meets the general objectives of an organisation.

CHAPTER 3: FINDINGS

Figure 2: The technological layout of Web 3.0



3.1 Introduction

In order to assess the impact Web 3.0 technologies will have on business operations, the first step will be to define the different technologies associated with Web 3.0. The technologies defined will offer specific opportunities or uses for an organisation. After obtaining an understanding of Web 3.0 technologies, COBIT control processes will be used to identify risks associated with Web 3.0 technologies. The impact the opportunities will have on the IT infrastructure, will also be considered when evaluating the risks. After the risks have been listed, controls will be identified to mitigate these risks.

3.2 Defining technologies associated with Web 3.0

According to Berners-Lee, Hendler and Lissila (2001), Web 3.0 will rely on a variety of different technologies, some of which still has to be created, while others are already, to a degree, being implemented on the Web as we know it. The following sections discuss some of these technologies.

3.2.1 Extensible Mark-up Language

Extensible Mark-up Language (XML) lets everyone create pieces of information, also known as tags or hidden labels. These tags are used to describe or explain certain parts of a Website or sections of text on a page. It acts as a medium through which mark-up languages can be created for specific applications. These tags of information can be used by other scripts or programs in very sophisticated ways if the script writer understands what the page writer used the tags for. XML provides a way for page writers to include extra tags of information on their pages, but does not explain what the tags are used for, which makes it hard for the script writers to use this information (Tim Berners-Lee *et al.*, 2001).

Unicode is an extensive way of defining characters electronically to ensure internationalisation of applications. It is based on similar principles as ASCII code, and is used by XML to describe characters.

3.2.2 Simple Object Access Protocol

Simple Object Access Protocol (SOAP) is a simple XML-based protocol that enables communication between different applications. Hyper Text Transfer Protocol (HTTP) is a simple protocol used on the Web to enable different machines with different operating systems and software to communicate with each other over the Internet (Rouse, 2005). One of the main characteristics of Web 3.0 technologies is internationalisation of Web languages and interoperability of all machines on the Web. Current Web applications run secure protocols, and HTTP has not been designed to bypass these firewalls, which lessen interoperability of new applications. SOAP uses XML and HTTP to communicate between applications and bypass firewalls.

3.2.3 Resource Description Framework

Resource Description Framework (RDF) is a mechanism through which information about data is captured. It acts as a mechanism for Web page writers to add semantic information to their Web pages. This type of data collected by RDF is called *metadata*.

RDF creates statements about particular resources on the Web by means of a triple expression in the form of subject-predicate-object. The subject represents the resource, while the predicate refers to an attribute of the subject, and the object is what is referred to in the predicate. By using the simple example “Josh likes chocolate”, “Josh” will be the subject, “likes” will be the predicate, and “chocolate” will be the object. This structure is the natural

way to describe the vast majority of the data processed by machines (Tim Berners-Lee *et al.*, 2001; Decker, Melnik, van Harmelen, Fensel, Klein, Broekstra, Erdmann & Horrocks, 2000).

RDF uses Uniform Resource Identifiers (URI) to specify subjects and predicates. URI's are used to identify all resources on the Web. After the information has been identified, the method of locating the resources is called Universal Resource Locator (URL). URL's specify where to obtain those resources (Wikipedia, 2013d).

It is clear that XML and RDF have some similar qualities on querying documents on the Internet. XML has the ability to query information in a document, while RDF has the ability to extract the “meaning” of information in a document, and query that which will be essential in the development of Web 3.0 (Berners-Lee, 1998).

3.2.4 Resource Description Framework Schema

Resource Description Framework Schema (RDFS) is an extension of the RDF vocabulary. It has the ability to collect a range of properties and relate the RDF classes and properties into taxonomies using the RDFS vocabulary. RDFS describes a wider range of classes and properties, and is used as a mechanism to describe information on the Internet into taxonomies.

3.2.5 Structured Query Language and Simple protocol and RDF query Language

Structured Query Language (SQL) is a mechanism that enables communication with a database. It is the standard language for relational database management, and has the ability to perform tasks such as retrieving data from a database, or updating a database (Melton & Eisenberg, 2001). It is a widely used standard on the Internet. Due to the complexity of data storage within RDF and RDFS, a more complex and integrated query language had to be developed. Simple Protocol and RDF Query Language (SPARQL) was created in order to enable RDF database manipulation. It is The Web Consortium (W3C) recommendation for an RDF query language and protocol, and has the ability to make RDF data available through a standard interface, and query it, using a SQL (Quilitz & Leser, 2008).

3.2.6 Ontology Web Language and Web Ontology Language for Services

According to Sowa (2009) ontology is the study of the categories of things that exist or may exist, and describing their relationships in a certain domain. For the Web, ontology is about extracting descriptions of Web information, and understanding relationships between Web

information. Ontology Web Language (OWL) is the language that enables a machine to process information contents on the Web in a universal manner. OWL was created to give machines, instead of humans, the ability to process and read information on the Web. OWL has a lot of characteristics similar to those of RDF, but is much stronger with greater machine interpretability, a larger vocabulary and a stronger syntax (Webschool, 2013). Similar languages have been developed in the past, but only for specific user communities (like the science and company-specific e-commerce applications). These earlier adoptions of ontology languages were user-specific, and not designed to be compatible with the architecture of the Web, not mentioning Web 3.0.

The ability of machines to harvest information and understand the meaning thereof, is a crucial characteristic needed in order to develop Web 3.0. OWL will create the opportunity for machines to adopt these characteristics and, through RDF linking, enables a Web where information is categorised by machines in a meaningful manner and in a universal format that can be queried by any other scripts (Horrocks, 2004).

OWL-S is an extended version of OWL, based on the same principles and annotation processes, but has a greater ability with respect to expressive properties, extends support for data types, enables metamodeling and extends annotation (Golbreich & Wallace, 2012).

3.2.7 Intelligent agents

One of the major features that need to be available in order for Web 3.0 to be more accurate and useful, is the establishment of interlinking data between data sets across the Web. Intelligent agents with the use of ontologies will enable interlinking. Intelligent agents are enclosed computer systems consisting of specialised computer architecture and programming (Lewis, 2008). These intelligent agents are programmed to function in a manner similar to humans browsing the Web. Agents will be omnipresent on Web 3.0, and will be able to harvest and collect information in a meaningful manner without human interaction. The precision and applicability of the information harvested and utilised by agents, will be greatly improved through the use of ontologies (Lu, Dong *et al.*, 2002).

The ability which OWL technologies provide to agents will enable them to create meaningful reasoning about information on the Web, which will equip agents with knowledge about data, and increase their intelligence and mobility. The current computing paradigm on the Web is based on the client/server initiative. With agents gathering more intelligence and mobility, the

paradigm will shift to agent based distributed computing. Agents will be able to fulfil their assignments autonomously and precisely by migrating from one site to another, carrying their codes, data, running states and intelligence (Lu, Dong *et al.*, 2002). Agents will act as an electronic assistant by automating repetitive tasks, intelligently harvesting and summarising complex data, and being able to learn on behalf of the user by analysing the users' interaction with the Web. The information gathered from this analysis, will give an agent the ability to make recommendations to the user (Gilbert, 1997).

Gilbert (1997) summarises the main characteristics of an intelligent agent as follows:

- Intelligent agents are **autonomous**, independent and are able to operate without user interaction.
- Intelligent agents are **goal-driven**, operating in accordance with specific purposes. The user will make this purpose known to an agent by setting different parameters through the use of scripts, programs, rules and planning methodologies.
- An agent is **reactive**, responding to changes in its environment in a timely manner without user interaction.
- Agents are **social**, being able to communicate, share and harvest intelligence from other agents.
- Agents are **customised** or **adaptive beings**, able to learn from previous experience and adapt to perform their purpose in a more efficient manner.
- Agents are **mobile**, which means that they are able to move between many different machines and devices.

Intelligent agents have been developed since 1997. Their ability to harvest information collectively and autonomously and to structure it has been limited due to the fact that they are not able to harvest information from the Web in a meaningful way, and reason with this information. With the introduction of technologies like OWL, intelligent agents will gain the ability to understand the information that they harvest and apply/communicate this information in a meaningful way.

3.2.8 Conclusion

As stated by Berners-Lee (2001) Web 3.0 is not a development of new protocols, architectures and infrastructures of the Web, but rather a calibration and expansion of already existing ideals and standards. The technologies discussed will form the core operatives to

enable Web 3.0, and mainly consist of scripts and programming codes/languages. The required infrastructure, usage, data and information are already available on the present Web 2.0 platform. These technologies will form the fundamental structures which will enable machines to exploit the rich content available on the Web.

The following illustration will give perspective as to where and how the technologies interact in order to form Web 3.0 (Shapovalenko, 2008):

3.3 Opportunities or possible uses for Web 3.0

3.3.1 Introduction

In present business and other environments, the Web is an essential resource, and Web 3.0, with metadata annotated information, will be even more vital for completing information based tasks. By combining the technologies discussed in section 3.2, the Web has the potential to become the location of every possible information resource, person, and organisation, and all the activities relating thereto (Sheth & Meersman, 2002). Through Web 3.0 and intelligent agents, processes will become more automated, producing information much faster and precisely, at an improved level of access (Bakshi & Karger, 2005). The enhanced ability Web 3.0 will offer to machines to categorise and add meaning to information, will increase the range of uses for the Web, and will bring forth new opportunities, to be elaborated on in the rest of this chapter.

3.3.2 Web services

One of the most important characteristics of Web 3.0 technologies is the ability to automate the process of describing and contextualising metadata within websites. An important resource Web 3.0 technologies will offer in this regard is automation of Web services. Web services, in this context, refer to websites which not only provide static information and allow the user to interact and contribute information, but also have the ability to create new Web services based on user preferences. According to Ankolekar, Burstein, Hobbs, Lassila, Martin, McIlraith, Narayanan, Paolucci, Payne, Sycara, and Zeng (2001) Web 3.0 technologies will enable autonomous locating, selecting, employing, composing and monitoring of Web services. Lu *et al.* (2002) state that the realisation of autonomous Web services will only occur once the following stages of automatic Web services have been developed:

- **Automatic Web service discovery.** This stage describes the ability to obtain information on Web services. The ability provided by Web 3.0 technologies to register semantic descriptions of Web services on a universal repository, will enable intelligent agents to harvest these descriptions, and migrate between different repositories to find the desirable Web service specified by the user. An intelligent agent can create a user profile by harvesting browser history information about the user. By integrating semantic information and the capabilities of intelligent agent automatic Web services, discovery will be possible.
- **Automatic Web service invocation.** One of the basic characteristics of current Web services is user interaction; without constant user intervention the usability of Web services deteriorates. Lu *et al.* (2002) state that automatic invocations imply that an intelligent agent will be able to perform basic tasks on behalf of the user depending on the parameters set for the agent. According to Hess and Kushmerick (2003) automatic Web service invocation will only be capable when each Web service is described by semantic metadata which is available in a machine readable format. Web 3.0 technologies offer the procedures needed to generate the necessary metadata automatically.
- **Automatic Web service composition and interoperation.** OWL technologies will provide a complex library of Web services with high level descriptions of objectives. Web service software can be written to manipulate these libraries and, together with highly specified objectives, enables automatic creation of new Web services in order to achieve the objectives (Martin, Burstein, Hobbs, Lassila, McDermott, McIlraith, Narayanan, Paolucci, Parsia, Payne, Sirin, Srinivasan & Sycara, 2004).

New Web services with the ability to autonomously publish, discover and invoke information from a variety of publicly available sources, shared through vast networks of machines and users, will contribute to a network with richer content.

3.3.3 Agent based information harvesting and distribution

Agent based distributed computing refers to the shift in the computing paradigm from information distributed through a client/server initiative, to information harvested and distributed autonomously by intelligent agents. Intelligent agents and agent based distributed computing are described in detail in section 3.2.6. According to Lange and Oshima (1999) the following advantages will be associated with the agent based computing paradigm:

- **Reduction in network load.** Intelligent agents will allow the users to package data or information and send it via the network to the host. The interaction needed to accomplish the task will be done on the host's system, and not over the network, as is the case with most distributed systems.
- **It overcomes network latency.** In manufacturing processes where latency on the system is unacceptable, and machines have to adapt in real time to changes in their environment, intelligent agents will be crucial.
- **Dynamic adaption.** Intelligent agents can adapt autonomously to changes in their environment. This enables them to allocate themselves throughout an entire network of hosts. In doing so they keep updating their configurations in order to solve specific problems.
- **Heterogeneous characteristics.** Intelligent agents are independent of computer and transport layers, and this enables continuous system integration.
- **Robust and fault tolerant systems.** The ability of intelligent agents to adapt to environmental changes means that they will be able to adapt to adverse situations as well. When a host within a distributed system shuts down, the agents executing on this system will be warned in advance, and will have sufficient time to migrate to other hosts, which will ensure a robust system.

3.3.4 Search engine capabilities

The traditional search engines lack coherence in two major areas, namely, the reliability of the resources, and the relevancy of the information found by the search engine. The reason these problems occur is due to the current structure of the Internet. Documents and information are linked via hyperlinks which are easily understood by humans, but not by machines (Shaikh, Siddiqui, Shahzadi, Jami & Shaikh, 2010). Natural language processing and Web 3.0 technologies will enable a search engine to organise information based on the context within the document, and not just recognition of phrases. This, combined with information collected by intelligent agents, will better define the users' preferences and make searches more powerful, precise and personalised than is possible with current algorithms (Verizon, n.d.).

Web 3.0 technologies will contribute to the creation of an intelligent search engine through the use of XML metadata tags, and queried information will be searched. The metadata gathered by XML will then be extracted into RDF format. This will form the database from

which information will be extracted. To make sure that data within this database remains relevant, the power of ontologies like OWL will be implemented. The data will be queried and retrieved by the use of SPARQL (Shaikh *et al.*, 2010). By utilising the different Web 3.0 technologies, semantic interoperability can be achieved by ontologies, while XML and RDF ensure machine comprehension.

RAF Technology (2004) listed the following advantages that might be associated with a semantic search engine enabled by Web 3.0 technologies:

- **Increased re-usability of information.** Web 3.0 technologies will enable re-use of information. According to Bürger (2008) this will lead to significant improvements in the manner content is created, and the adaptability of content on the Web. This will in effect increase the quality and consistency of information, and reduce the cost of creating, maintaining and altering the information.
- **Advanced co-operation and expert findings.** Through the use of Web 3.0 technologies search engines will be able to resort to ontologies, to not just reason with queries, but also to collect prior knowledge from resources supplemented by users. With Web 3.0 technologies users will be able to query information by using natural language. The query will be translated into its semantic representation which will enable the engine to search semantic resources that match this query. In instances where the query has more than one answer, the answers will be congregated according to their semantic meaning. Increased co-operation between wider ranges of resources, will eliminate ambiguity, and will increase relevancy and precision of search results (Melo, Rodrigues & Nogueira, 2012).
- **Knowledge exchange and time saving.** Web 3.0 technologies will enable machines to reason with data in a manner similar to human reasoning. This will enable machines to convert large amounts of data into useful information at much greater speed than has ever been possible. The information harvested by machines will then be queried by users which will turn the information into knowledge, which will be available and has the ability to be shared between all machines and users on the Web.

3.3.5 Business intelligence

Business intelligence (BI) or big data as described by Herschel and Jones (2005) is all types of technologies which enable organisations to collect and analyse raw data and convert it into

useful information in order to improve decision making. Hameed (2004) defines BI as finding hidden, essential and decision relevant information within large populations of economic and business data. BI worked well in the early developing stages which were characterised by minimal electronic data and minute resources. With the exponential growth in the availability of electronic data, the analysing of vast amounts of electronic data and the complexity thereof became problematic. Organisations were forced to obtain analysts with domain expertise to analyse the data manually (Guess, 2013).

Web 3.0 technologies will enable documents to be annotated with metadata, and these annotations will increase the amalgamation and accuracy of data extraction. Information extraction through natural language processing tools will be vital in order to be able to use the massive amounts of semantic information (Horacio, Funk, Maynard & Bontcheva, 2007). Web 3.0 technologies like OWL will enable a platform by which Web resources will be representative in a heterogeneous manner. Ontology will act as the unified structure by which information and the underlying semantics are represented universally (Davies, Fensel & van Harmelen, 2002). With the combination of metadata and ontology languages the Web will be able to offer a more qualitative service in collecting business intelligence.

The real ability of BI will not be realised until such time as Web 3.0 technologies are developed and functioning effectively. Web 3.0 will enhance the following benefits associated with the implementation of BI:

- **Reduced cost of IT infrastructure.** Cost will be reduced by eliminating big, investment intense data warehouses which in the past were essential for storing huge amounts of data before it could be extracted and converted into meaningful information. Redundant extraction processes performed in order to harvest data from data warehouses, will be eliminated, which will further reduce infrastructure cost (Watson & Wixom, 2007). The need to hire personnel with domain expertise will be eliminated, which will reduce labour cost as well.
- **Opportunity to increase effectiveness of e-commerce.** There is great potential for business intelligence to make useful contributions to e-business (including e-commerce) in particular the ability to track the users' browsing behaviour down to individual mouse clicks. It will enable suppliers to customise their product message for an individual customer (Zhong, 2003). Organisations spend large amounts of money on internet marketing. These marketing campaigns rarely reach the targeted

audience. Web 3.0 technologies will enable organisations to apply targeted marketing, creating a Web environment where consumers receive personalised advertisements while browsing the Web.

- **Time saving for data suppliers and users, and the reduction of information bottlenecks.** Through the use of Web 3.0 technologies data can be supplied and used more efficiently. Users can extract reports when they need it without specialised support from IT or financial personnel. Ontologies will enable users to extract new reports that match their exact requirements.
- **Timely and informed decision making.** Web 3.0 technologies possess the ability to autonomously integrate and structure data, and convert it into qualitative information. This information will be readily available for users based on their preferences and parameters. Extraction of data by machines from multiple sources with far greater efficiency and precision, will support organisations in making better decisions based on relative and accurate information (Watson & Wixom, 2007). Furthermore, intelligent agents can be programmed and deployed to harvest information autonomously based on rules set by the user.

3.3.6 Knowledge management

A considerable overlap exists between business intelligence and knowledge management (Eckerson, 1999). Business intelligence refers to the activities performed by end users to extract and process data into information through various analytical and collaborative tools in order to review historical activities. It is described as the process of turning data into information and, over time, into knowledge that can be fed back into business. Knowledge management focuses on the extraction of contextual information and rationalisation thereof through the experience and thought process of the specific end user. Knowledge management is the creation of new information based on the users' experience and understanding of the specific information. Herschel and Jones (2005) describe knowledge management as the improvement of a users' comprehension in a specific area of interest. This enables an organisation to gain a competitive advantage by analysing its own experience. Davies (2000) explains that the discipline entails different tools, techniques and processes to manage organisational knowledge and intellectual assets.

The major pitfalls associated with the implementation of efficient knowledge management systems are that organisations fail to align the system with its strategic objectives; create

repositories without managing the content, and harvest relevant information from a variety of resources. Because of the vast amounts of data available, and the need for human reasoning, organisations tend to focus on managing knowledge within organisational boundaries, with no information gathered from outside sources.

Web 3.0 technologies will enable organisations to deploy intelligent agents with specific parameters to perform this task. Ontologies will enable machines to structure relevant data into machine understandable information which can be extracted by intelligent agents. The process of knowledge management will be mainly automated, and this will increase the amount and accuracy of the data that can be processed into knowledge.

New business opportunities can be generated by collecting knowledge. The following key benefits are associated with efficient knowledge management (Oracle, 2011):

- **Reduced research time.** Cost can be reduced by lowering the call handle time and ensuring a better customer experience. In order for this to be achieved, agents need to be able to query any information available on a multitude of sources, including product manuals; marketing collateral; corporate policies, databases and case notes. Data mining to this extent can be time consuming, inaccurate and overall inefficient. Web 3.0 technologies will enable organisations to automate this process by assigning it to intelligent agents. With technologies like OWL, agents will have the ability to extract information from a vast array of sources that will be relevant to the specified query, and by doing so reduce research time. Furthermore intelligent agents will be able to store the queried results, which will enable instant recalling of specific queries.
- **Business benefits.** With effective knowledge management techniques organisations can benefit from improved management which will contribute to organisational success such as increased productivity; sales growth; cost reduction; improved employee development and retention; improved customer satisfaction, and expansion of social and intellectual capital with external stakeholders (Edvardsson & Durst, 2012).

3.3.7 eLearning and research

According to Naeve, Lytras, Nejdl, Balacheff and Harding (2005) Web 3.0 technologies and their ability to express meaning to data, will open an area of exploitation in eLearning and

research. The facilities provided by Web 3.0 technologies will enable learners to create, annotate, share and discuss content over the Web (Ghaleb, Daoud, Hasna, ALJa'am, El-Seoud & El-Sofany, 2006). According to Sampson, Lytras, Wagner and Diaz (2004), Web 3.0 applications will enable the creation of hypermedia systems. These hypermedia systems are portrayed as silos of information with the ability to adapt to the changes in its environment. The ability for a database to adapt is a crucial factor in the area of eLearning, especially taking into account the different needs of learners to propose learning goals, learning paths and help students to orientate themselves in the eLearning systems, and support them during their learning progress.

Ghalebi *et al.* (2006) believe that with the introduction of an eLearning framework with the inclusion of ontology based properties and hierarchical semantic associations, the possibility of creating an eLearning system with the capabilities of adapting and intelligently supporting learners, is inevitable. Introducing intelligent agents into this scenario will further enrich information created and shared by learners, and will in its universal format be integrated with homogeneous information and redistributed throughout the Web.

According to Koper (2004) the following benefits can be expected when eLearning is integrated with Web 3.0 technologies:

- The delivery of a time and cost effective, Web based curriculum with incorporated multimedia, intractability and the ability to adapt to the learner's specific characteristics.
- The presentation of courses by a variety of authors can be preserved. These teaching patterns can then be shared between different authors, and effective learning and teaching patterns can be created and adapted for different learning scenarios.
- Reduction in time and cost to develop new Learning Management Systems.
- Semantics and ontologies built into the course can be interpreted by intelligent agents in order to support the management of activities and workflow, and also ensure that relevant resources are used during learning activities.
- Time, effort and cost to adapt a course to an individual learner's characteristics, can be reduced through the ability of Web 3.0 technologies to autonomously adapt to changes in its environment.

- Better and more relevant research can be performed on effective learning designs due to the semantic structure of courses, and the ability to autonomously compare a variety of resources with ease.

3.3.8 Inbound marketing

With traditional marketing, organisations tend to blindly market their product to all customers available, even if they have no interest in the product. This type of marketing is known as outbound marketing, and focuses on the number of customers reached, rather than ensuring that interested customers are reached. Examples of this type of marketing include sales flyers, spam emails and telemarketers (Prescott, 2012). With the ever growing activity in internet economy, this method is becoming obsolete. A new type of marketing, called inbound marketing, is emerging. According to Prescott (2012) inbound marketing involves the distribution of information to consumers who value the information, which builds confidence and trust between the consumer and the company. The method of advertisement is mainly in an electronic format, and consists of a wide range of content marketing including blogs; videos; eBooks; eNewsletters, whitepapers and social media marketing. The main objective of inbound marketing is to target specific consumers based on their semantically related market segments, even if they are unaware of the product (Wikipedia, 2013a).

Web 3.0 technologies and information harvested by semantic search engines, will enable marketers to extract valuable historical consumer preferences based on their historical browsing activities on the Web. This information can be used to target specific market segments, and build an electronic relationship with consumers by personalising their economical browsing experience. The following benefits can be expected when incorporating Web 3.0 technologies with inbound marketing:

- **Brand awareness and credibility.** The more mediums - social networks, blogs, videos - you have through which your brand is being advertised, the bigger the opportunity to be hit by a consumer. While your hits accumulate, your position on the Google search list increases. High rankings on a Google search list will subconsciously increase consumer trust in your brand, which will increase brand credibility (Optify, 2013).
- **Cost reduction benefits.** According to Optify (2013) leads from inbound sources cost between 50%-60% less than leads from outbound sources. The main reasons for

this are cutting cost spent on third party marketing by using the resources available on the Web instead.

- **Increased quality of leads.** The quality and sale ratio of the consumers that visit your Website is much higher, due to the fact that consumers looking for a specific solution, are provided with the effective, informative and relevant information they are looking for (Optify, 2013). With inbound marketing you create content that add value for consumers, instead of dumping huge amounts of data, and hoping consumers will respond.

3.3.9 Conclusion

The main theme present throughout this section is the ability of Web 3.0 technologies to autonomously harvest data from the Web, and reason with it in a meaningful way. Machines adopting humanlike characteristics with the ability to collect and distribute data at a relatively far greater speed and accuracy, will create an opportunity for consumers to utilise the full capabilities of the Web.

3.4 Risks associated with Web 3.0

3.4.1 Introduction

Web 3.0 technologies create the opportunity for collaborative and autonomous integration of data on the Web. Autonomous machine communication, harvesting of data and creation of information, present serious risks that need consideration when evaluating Web 3.0 technologies (McGraw, 2008). Rudman (2010) explains that the risks associated with the different stages of Web evolution, are incremental. Vulnerabilities which were present during the first generation of the Web, had an impact on the second generation as well. The same notion will be applicable to the third generation of the Web. Some of the homogeneous vulnerabilities that organisations are, and will be, exposed to, which were also prevalent to previous Web generations, are (Rudman, 2010):

- Unauthentic electronic intrusion.
- Unwanted application performance due to continuous updates.
- Over-reliance on services offered by third parties, or only relying on server side security.
- The loss of confidential and personal information due to malicious attacks.
- Unproductive use of organisational resources.

- Non-compliance with regulatory governance, and the possibility of loss due to legal action.
- Shortage in experienced technicians to ensure effective operation and monitoring of complicated systems and applications.

The next part of the paper explains the risks incrementally associated with Web 3.0 technologies.

3.4.2 Unauthorised access to sensitive information

The exponential growth and availability of information on the Internet, and the new technologies offered by Web 3.0, will make data a crucial information resource. The ability of Web 3.0 technologies to personalise Web usage, and intelligent agents to harvest browsing history and personal information in order to automate the Web experience, will bring forth a new level of privacy concerns. In order for the vision of Web 3.0 to be successfully automated, protocols need to be deployed within Web 3.0 technology in order to address security and privacy issues (Kagal, Finin & Joshi, 2003). According to Nematzadeh and Pournajaf (2008) securing the Web is not just preventing unauthorised access, but also the prevention of unauthorised modification of data and use of resources.

Kumar, Prajapati, Singh and De (2010) divide unauthorised access and data manipulation into four categories:

- **Unauthorised access.** The intrusion and capturing of sensitive information on a system by an entity without authentication. A system with vulnerabilities will be exploited to gain unauthorised access. Many known and unknown authorisation vulnerabilities exist. Some associated with Web 3.0 technologies is when no authentication whatsoever is being used, or when password authentication is present, but it gets passed in plaintext format through SOAP headers. Another threat is when basic authentication is being implemented, but the data is transferred over unencrypted channels, or when the system accepts default passwords.
- **Parameter manipulation.** This refers to the tampering with data while it is being transferred over a network. It occurs when an unauthorised entity has the ability to intercept data being transferred between the consumer and the publisher. Some of the vulnerabilities which exist on systems which will increase the probability of

these types of attacks, are data packages that are not digitally signed or encrypted to provide privacy and tamper proofing before being transferred over a network.

- **Network eavesdropping.** This refers to the ability of an unknown third party to listen in on conversations on a network and obtain confidential information without the knowledge of the communicators (McGraw, 2008). This is usually accomplished by using monitoring software to obtain privileged information contained in SOAP headers. Kumar *et al.* (2010) stress the fact that systems are more prone to attacks of this type if the system contains vulnerabilities like minimal encryptions on both message and transport levels, or if credential data is stored in plaintext in SOAP headers.
- **Message relay.** This type of attack enables an unauthorised person to intercept data sent over a network, and relay it back to the publisher. The attacker does not have to know what the content of the message is to be able to perform this. Generally the attacker will change crucial information in the message, like the delivery address, and then relay it back to the publisher without the knowledge of the consumer. Vulnerabilities in a system that might increase the risk of an attack, include messages without ID numbers to ensure that duplicate messages are prevented, unencrypted messages and messages that are not digitally signed.

Unauthorised access to confidential information has been a predominant risk since the development of Web 1.0. With the integration and personalisation capabilities of Web 3.0 technologies, the risk of unauthorised access will increase exponentially.

3.4.3 Hyper-targeted spam

Hayati, Potdar, Talevski, Firoozeh, Sarenche and Yeganeh (2010) define spam as the unsolicited distribution of large amounts of content via a network to a variety of consumers without their consent. He elaborates that spam has the ability of carrying infected scripts like malware, adware and viruses, which can be distributed in many formats including email, instant messaging, Web pages and Internet Telephony. These types of spam attacks have been prevalent in the historic evolution of both Web 1.0 and 2.0.

The ability of Web 3.0 technologies to integrate and link vast amounts of available metadata in a machine interoperable format, will create opportunities for a new enhanced form of spam attacks. According to Hasnain, Al-Bakri, Costabello, Cong, Davis and Heath (2012), the ultimate goal of spammers to distribute unsolicited content over networks, will not be

affected by the new Web 3.0 technologies, but the method of distribution and the intensity thereof, will. Hasnain *et al.* (2012) and Ferrel (2008) describe the methods of exploitation of the platform provided by Web 3.0 technologies, as follows:

- **Application pollution.** Applications running within Web 3.0 will use the entire Web's resources as a database. This creates an opportunity for spammers to infect a universal resource that acts as a specific database for a specific application. With the infection of an application's database, spam can be distributed directly inside the running application.
- **Improved ranking.** Ranking is the method applied to determine what rank a search result will obtain when entered into a search engine. The higher the rank, the better the chance of being selected by a consumer. Web 3.0 technologies will empower search engine capabilities, which will create an opportunity for spammers to manipulate the ranking of malicious resources by creating triples containing malicious literal values that will be able to influence term based metrics. Complicated algorithms in co-operation with linked data are used to calculate the rank of the resource. Spammers will also attempt to exploit these algorithms by creating fake external links to resources in order to improve the resource rank.
- **Hiding.** One of the main characteristics of successful spammers is the ability to hide malicious content from anti-spam software. Web 3.0 will be based on open source which will enable intelligent agents to automatically harvest information about anti-spam software, and will empower spammers to improve their method of hiding malicious content.
- **Personalisation of Web content** will enable spammers to gather more private and precise information about users of organisations, and attack them in ways that will make differentiation from legitimate communication increasingly difficult.

3.4.4 Identity theft and social phishing

Phishing is a socially engineered crime through which confidential information is harvested by an unauthorised party impersonating a trusted third party (Whittaker, Ryner & Nazif, 2010). A similar threat is identity theft which is the process of harvesting personal information with fraudulent intent by means of exploiting information available on electronic communications mediums (Lynch, 2005). Both these risks existed previously on Web 2.0, but

the precision and volumes of these threats will increase exponentially with the introduction of Web 3.0 technologies.

The main threat is the ability of script writers to exploit sensitive information distributed in metadata, described by machine understandable ontologies, and harvested autonomously by intelligent agents. Farkas and Hunhs (2002) support this assertion by describing an incremental threat attributed to Web 3.0 technologies:

- **Inference attack** is a form of intense data mining where confidential information is harvested and disclosed by integrating non-sensitive data with metadata. Web 3.0 technologies will introduce richer metadata, and with ontologies the integration capabilities of metadata will increase. With the increased integration of metadata, consumers will lose track of sensitive data available on the Web, and where it is stored, and this will lead to an increase in the precision and volume of inference attacks.

3.4.5 Autonomous initiation of instructions and malicious script injections

Web 3.0 technologies are based on different levels of languages, each with its own individual characteristics. The most common attack on Web languages takes place in the subset of Query/Update languages (Orduña, Almeida, Aguilera, Laiseca, López-de-Ipiña & Goiri, 2010). The most widely used query language in the development of Web 3.0 technologies is SPARQL. Orduña *et al.* (2010) introduces three new types of query injections that will be associated with Web 3.0 technologies:

- **SPARQL injections** are a technique used by malicious attackers to take advantage of vulnerabilities occurring in Web applications by gaining unauthorised access to the back end layer of a database by passing non-validated SPARQL commands through a Web application (Su & Wasserman, 2006). Attackers manipulate the execution of Web application commands by structuring specific queries that enable them to harvest sensitive information within the applications' database.
- **Blind SPARQL injections.** The query languages used with Web 3.0 technologies will consist of complicated and high level structures which will make retrieval through injection attacks much more difficult (Orduña, 2010). Through blind SPARQL injections the attacker queries the database, and receives Boolean result.

By querying the database repeatedly, the attacker can harvest sensitive information through true and false error messages provided by the database (Hotchkies, 2004).

- **SPARUL injections.** SPARUL is the update version of SPARQL, and allows not only reading query abilities, but writing as well. This creates a new threat for manipulations and extraction of data from a database, since the entire ontology can be modified through queries (Orduña, 2010).

Injection of non-validated commands in a query language has been a pre-existing threat in Web 2.0. With the development of new query languages for Web 3.0, the threat needs to be re-evaluated.

3.4.6 Development of ontologies

Ontologies being the carriers of meaning of information available on the Web, will need to be developed to be able to interpret unified meanings of information in order to integrate information gathered from a variety of sources. An adequate infrastructure needs to be set in place to support ontology development; mapping; annotations referring to them, control over adjustments and creation of new ontologies (Mercer, n.d.).

Benjamins and Contreras (2002) explain that the major concerns that need to be addressed in order to manage the risks associated with the development of ontologies, are the creation of kernel ontologies which will act as a unified top level dictionary. The ontologies development process will also need the necessary methodological and technological support and configuration management in order to control the creation of different versions of ontologies, and to manage the association between the ontologies and annotations.

The creation of a new technology like ontologies also poses the threat of exploitation due to inefficient knowledge of the subject. Like any technology in the beginning of its development phase, script writers will try to take advantage of vulnerabilities prompted by inexperience with the technology. Vulnerabilities include, but are not limited to, hidden malicious script within ontologies, and manipulation of ontologies in order to obtain sensitive data.

3.4.7 Proof and trust standardisation

Due to the ability of Web 3.0 technologies to autonomously harvest and integrate data and convert it into information, all statements on Web 3.0 need to be considered as claims before they can be trusted (Gil & Artz, 2007). Only when these claims have been established, should

trust be put in the information provided. In order to be able to trust harvested information, the source of the information as well as the policies available on the source, needs to be obtained and analysed (Medić & Golubović, 2010).

Intelligent agents can use both the context and reputation of sources to determine the level of trust that can be put in a source (Gil & Artz, 2007). Intelligent agents will be able to communicate among themselves without human interaction to determine if a source (i.e. the agent of the source), can be trusted. This creates an opportunity for malicious attackers to write scripts which impersonate a trustworthy agent, and enable them to perform unauthorised actions and inject harmful scripts.

Web 3.0 technologies will rely heavily on semantic tagging. Script writers can manipulate semantic tagging by providing inaccurate information, and by doing so improve their Website ranking. With higher rankings more users will visit these Websites based on falsified information, which can be infected with various types of malware and harmful scripts (Mercer, n.d.).

3.4.8 Internationalisation – multilingualism

The challenge of sharing information from different geographical areas in a common language understandable by all participating entities, has been prevalent in Web 2.0. New technologies arising from Web 3.0 will also be affected by the risk of multilingualism. According to Benjamins *et al.* (2002) multilingualism will affect some of the following areas of Web 3.0 technologies:

- **Ontologies** will be one of the cornerstones of Web 3.0, and developers will need to develop ontologies in their native language.
- **Annotation** and the description of content will be a bigger challenge since most of the Web community will take part in annotating its specific content. These annotations will have to be in detail and precise in order for Web 3.0 to realise. Consumers will only be able to become contributors if proper support is created to enable them to annotate in their native language.

Language boundaries will suppress the ability of consumers and contributors to describe and integrate content. This will increase the risk of non-interoperability and miscommunication between applications and intelligent agents, which will defeat the purpose of Web 3.0.

3.4.9 Conclusion

Many of the risks identified in this section were prevalent in Web 2.0, but due to the addition of new technologies with original and unknown structures, additional risks will arise. Organisations are usually quick to adopt new technologies based on the benefits and opportunities they might possess, but fail to recognise the threats associated with these technologies. New controls and methods of regulating activity on Web 3.0, will need to be adopted in order for these new technologies to operate effectively and accurately.

3.5 Safeguards and controls to mitigate risks

3.5.1 Introduction

Web 3.0 will be an environment where data and information will be shared openly and interactively. Information will be much more valuable to organisations and consumers, and it needs to be treated and protected as an asset (Tarrant, Hitchcock & Carr, 2011). The consumption of information by machines will affect the level of control an organisation can exercise over securing valuable information on the Web (Middleton, Halbert & Coyle, n.d.). The following section will discuss controls that should be implemented in order to mitigate the risks associated with Web 3.0 technologies.

3.5.2 Controls

Some of the controls listed are inherited from previous Web generations. Due to the modification of the underlying technological structures and processes, these controls need to be revisited and modified in order to mitigate the new risks. The threats can be controlled through the use of technological methods with the inclusion of an administrative component (Rudman, 2010).

3.5.2.1 Technological control

The following technological controls can be implemented to reduce the risks posed by Web 3.0 technologies:

- **Encryption and authentication.** Communication between a Web server and a consumer is controlled by input and output parameters. In order to ensure secure transmission of data these parameters need to be encrypted. This can be accomplished by using a semantic mark-up that specifies the security characteristics of the Web servers' input and output parameters (Kagal, Paolucci, Srinivasan,

Denker, Finin & Sycara, 2004). This will enable the data to keep its structure while not revealing the values, after which matchmaking services can select the service required by using this meta-information. Lee and Whang (2006) stress the fact that encryption mechanisms like Secure Sockets Layer (SSL) and Transport Layer Security (TLS), which are commonly used during transmission of HTTP protocols, are not sufficient for XML or RDF transmissions. XML Encrypt (XMLEcn) and XML Signature (XMLSig) are standards used to encrypt XML data and ensure that data which is transmitted, is authenticated through the use of digital signatures. Partial RDF encryption (PRE), as suggested by Giereth (2005), recommends an algorithm which encrypts fragments of RDF content to ensure secure transmission of data.

- **Access control.** Web 3.0 technologies will grant access to resources through SPARQL query language, which will also be the main exploit malicious attackers will use to gain unauthorised access. Social Semantic SPARQL Security for Access Control (S4AC) discussed by Villata, Delaforge, Gandon, and Gyrard (2011), is an access control vocabulary for SPARQL query language. It enables users to invoke access control policies for their RDF data by using a SPARQL 1.1 ASK clause that enables them to specify certain conditions within metadata tags that need to be met before access is given to resources. ROWLBAC (Finin, Joshi, Kagal, Niu, Sandhu, Winsborough & Thuraisingham, 2008) and SecurOntology (García-Crespoa, Gómez-Berbísa, Colomo-Palacios & Alor-Hernández, 2011) are more methods to ensure secure access of OWL ontologies which can be implemented to mitigate access control risk.
- **Guaranteed e-delivery.** This method promises the secure delivery of electronic information, and ensures through follow-up controls that the information has not been tampered with during transmission. It is based on the combination of secure hosting and e-mail notifications. The recipient of the information will receive an e-mail that informs him that information has been sent, and that delivery is pending, while the sender will receive notification when the information has been retrieved. This enables crosschecks of information sent electronically (Gilbert, Abrams, Linden, Mogull, Orans & Wald, 2001).
- **Effective spam filtering.** The ability of ontologies to enable a machine to understand and reason with content, creates an opportunity to filter incoming and

outgoing data more effectively. Youn and McLeod (2007) implemented this control by mapping a decision tree into an ontology, thus enabling a server to understand incoming and outgoing messages, and based on rules set, filtering out spam emails. Eyharabide and Amandi (2012) introduced a next level of integration between the use of ontologies and spam filtering by not only using ontologies to filter spam, but also to personalise filter based on user preferences harvested by ontologies.

Dietzold and Auer (2006) suggest the implementation of a Lightweight Framework for Access Control which consists of an information query filter that is based on the quality and trust properties of resources. The framework controls access through a query engine that is limited by a rule processor which decides whether the query filter can trust a resource. The implementation of a Semantic Data Crawler which only harvests documents and information from predefined semantic Web data sources, can also assist in filtering out data retrieval from untrustworthy and malicious resources (Lašek & Vojtáš, 2011).

- **Anti-malware software.** Anti-malware software including anti-spy and anti-virus software, should be installed in order to eliminate the threat of malicious infections of a system. The software should be implemented to enable protection of both inbound and outbound electronic transmissions (Rudman, 2010). The implementation of a structure like Taiwan Malware Analysis Net (TWMAN) as suggested by Huang, Lee, Kao, Tsai and Chang (2011), will mitigate the risk of infections associated with Web 3.0 technologies. TWMAN consists of two intelligent agents, a malware behavioural analysis agent and an ontology agent. By integrating the information collected by the ontology agent, the malware behavioural analysis agent collects malware behavioural information and builds a malware behavioural ontology with malware behavioural rules. This creates a ubiquitous software agent that examines malware behaviour, and autonomously creates rules to protect the system from infection in real time. Chiang and Tsaur (2010) introduce the same concept of ontology based malware protection for the safeguarding of mobile devices.
- **Monitoring of composite events.** Rudman (2010) and Vaculín and Sycara (2007) exploit the abilities of Web 3.0 technologies by enhancing the monitoring process of complex events within a Web service. Monitoring of composite events will simplify

the process of sharing events and content between agents, and will contribute to the standardisation and internationalisation of Web content. User history logs that define all types of network activity, which includes bandwidth usage, sites visited and files downloaded, should be kept and reviewed regularly.

- **Network and underlying infrastructure security.** Most of the security surrounding access control is focused on the application domain. Action needs to be taken to ensure that the users' system also protects the transmission of electronic information. Foley and Fitzgerald (2008) suggest the implementation of firewall agents which act like intelligent agents with parameters set to support firewall configuration. The firewall agents will negotiate the firewall settings, controlling access based on a knowledge repository that is gathered from ontologies. This repository will be constantly updated and controlled by facts collected by agents as they harvest information from new knowledge and inferences.
- **Validation of input.** The most common attack to bypass input validation is SQL injections, which grant the attacker unrestricted access to database information. Halfond, Viegas and Orso (2006) suggest the implementation of a New Data Validation Service (NDVS) using Web 3.0 technologies. The NDVS consists of five components, namely a RDF annotation; an interceptor; a RDF extractor, a RDF parser and a data validator. The process of validating input starts by using ontology to describe all the data in the Web application through RDF annotation. When the user requests a HTML, the interceptor will intercept it before it gets processed at the server side. The RDF annotations are extracted from the RDF ontology by the RDF extractor, and compared to the user inputs by the validator to ensure valid inputs. If the validation is correct the request is processed.

3.5.2.2 Keep users and developers informed about the risks

Many of the risks identified in section 3.4 directly correlate with the lack of knowledge about these risks. The development of new technology is always accompanied by new unknown risks, and developers as well as consumers need to be educated and made aware of these risks. Shabajee (2006) and Rudman (2010) describe areas in which consumers and developers need to be educated:

- **A better understanding of the issues.** Both consumer and developer need to understand the risks arising from Web 3.0 technologies. Collaboration is needed

between the two parties to ensure that not only technical solutions are implemented, but consumer contributed solutions like Web interfaces, ease of use of applications and informative applications, are investigated as well.

- **Developers design methodologies.** Designers must be aware of the preceding risks before they start developing Web applications. During development stages technical solutions must be integrated into the design of the application to ensure secure and accurate execution of Web applications.
- **Education of consumers.** Consumers need to be educated in a wide range of issues surrounding Web 3.0 technologies, which includes, but is not limited to, technical understanding, identification of potential risks, and social rules and expectations. This can be introduced through the use of different approaches, like long term learning and maintenance campaigns, or by incorporating it into Web interfaces, which offers contextual tours to consumers to highlight risk areas within the application. Consumers also need to be educated about the major safeguards that are associated with the adoption of new technologies, like the identification of risks relating to the new applications; refraining from interacting with suspicious applications and attachments of emails from unknown sources, and using security features embedded in applications, browsers and underlying infrastructure (firewalls, anti-malware software).

3.5.2.3 Policies and guidelines controlling use

A predominant threat when adopting a new technology, is users engaging in these technologies without preliminary training and guidance as to what the technology entails, and why there are risks associated with it (Rudman, 2013). Organisations need to adopt regulating policies and guidelines to ensure users are educated and informed on how and why they are allowed to use certain technologies. When adopting these policies, organisations should not only consider written policies, but also automated policy creation through the use of semantic technologies. Policies implemented should not only support the organisations' strategic objectives, but also comply with regulatory governance. The policies should be clear and communicated to all levels of employees in a non-technical language. The policies should be written in a manner which makes it adaptive to changes, and it should be reviewed and adapted by top management on a regular basis (Rudman, 2010).

3.5.2.4 Setting electronic parameters

Kagal *et al.* (2003) suggest the implementation of distributed policy management through the use of a semantic policy language. This policy language will be based on ontologies written with specific parameters. The language will have some domain independent ontologies, but will also require specific domain ontologies. The language will consist of two constructs that will be able to select meta-policies, which will be invoked to resolve conflicts. The first construct is a modality preference (negative over positive), and the second is priorities construct (when there is more than one policy applicable, this construct will invoke the policy that enjoys priority). The use of ontologies to create policies will enable policies to be much more adaptive to real time changes, and by integrating it with intelligent agents, ensure that policies are more effective and applicable.

3.5.3 Conclusion

When considering the adoption of new technologies, organisational leaders are always eager to adopt the new technologies based on the opportunities they might offer. With the adoption of all new technologies new risks will arise which are rarely taken into account by organisational leaders when making these decisions (Hall & Khan, 2002). The risks associated with the adoption of Web 3.0 technology as stated in section 3.5.1, will be lowered to an acceptable level by implementing the controls mentioned in section 3.5.2.

CHAPTER 4: CONCLUSION

Modern organisations operate in a highly technological environment where technology plays a vital part in accomplishing the objectives set by organisational management. The methods by which the underlying technologies support the organisational goals, evolve rapidly and continuously. The need for organisations to adopt new technologies is crucial for keeping a competitive advantage, and exploiting the opportunities these technologies present. The introduction of Web 3.0 technologies will create new opportunities that will assist organisations in reaching their objectives.

With the adoption of new technologies, developers and consumers - including organisational management - tend to focus on the benefits, and ignore the risks associated with the implementation of these technologies. When analysing the impact these technologies could have, organisations should consider the risks at an operational level and implement controls to mitigate these risks.

The research shows that in order to understand the true impact of implementing new technologies, the underlying infrastructures that support these technologies, must be defined. COBIT 5 was used as a governance framework to identify the risks associated with Web 3.0 technologies and to implement control processes that can lower the threat to an acceptable level. Web 3.0 is not a separate or isolated technology, but rather a compilation of already existing principles amalgamated with new programs and scripts. These new technologies create an array of new opportunities summarised by the following characteristics:

- Overall increased collaboration between consumers, developers and machines. With Web 3.0 technologies enabling machines to read, understand and reason with information on the Web, information will become integrated and precise, readily available, and will become more valuable to the consumers of the information.
- Autonomous characteristics of Web 3.0 technologies will lighten the work load of data management, and enable new intuitive and personalised Web services.
- Web 3.0 technologies' ability to integrate and structure data autonomously, will increase the accuracy and availability of research data repositories. This will increase knowledge management, and enable more effective and collaborative research with less common restrains (such as language barriers).

- Intelligent agents harvesting personal habits and information of consumers, will create a personalised Web experience which will amount to countless opportunities for inbound marketing schemes.

The underlying technologies creating the opportunities are accompanied by risks specifically linked to these technologies. The main risks identified during this stage, are as follows:

- Unauthorised access to sensitive data, or data manipulation by unauthorised persons.
- New and more complicated electronic attacks, such as SQL injections, malware, hyper targeted spam and internet ranking manipulation.
- Personalisation of Web content creates a situation where personal and sensitive data will be more widely available on the Web, thus creating an increased risk of identity theft and social phishing.
- The development and standardisation of new Web ontologies and languages increase the probability of releasing inferior or easily targeted software and application, due to a lack of knowledge and insufficient testing for risks associated with the technology.

Safeguards which need to be implemented before Web 3.0 technologies are adopted in order to ensure that the risks associated with Web 3.0 technologies are mitigated to an acceptable level, include:

- A multilayer approach of technical and non-technical safeguards should be implemented. Technical safeguards include encryption and authentication; anti-malware software; physical and logical access controls; effective filtering and monitoring, and validation controls.
- Non-technical safeguards include ensuring that users are educated continuously about the underlying risks associated with the use of Web 3.0 technologies, and the communication of methods on how to avoid threatening situations.
- A policy regarding the use of Web 3.0 technologies should be implemented that pins down responsibility, and elaborates on what actions are expected from consumers when using Web 3.0 technologies.

Table 1 maps the incremental risks associated with Web 3.0 technologies identified during the research, and possible safeguards that can be implemented to mitigate these risks:

Table 1: Risks and safeguards associated with Web 3.0 identified:

[illegible]

The research shows that it is crucial for organisations to understand the underlying infrastructure of new technologies, and what opportunities they present. After getting a proper understanding of Web 3.0 technologies, organisations need to identify the risks associated with the implementing of these technologies.

Since Web 3.0 technologies are still in the developing phase the opportunities for future research is emanate. Prospective research based on the topics discussed in the research conducted can include further analysis of the impact Web 3.0 technologies might have on business imperatives on a strategic level. It will be able to conduct this type of research once more resources become available on the topic.

REFERENCES

- Alpert, J. and Hajaj, N. (2008), *We knew the Web was big*. Available at: <http://googleblog.blogspot.com/2008/07/we-knew-Web-was-big.html> (accessed 19 July 2013).
- Anderson, A. (n.d), *10 Most Important Business Objectives*, Demand Media. Available at: <http://smallbusiness.chron.com/10-important-business-objectives-23686.html> (accessed 9 September 2013).
- Anderson, P. (2007), *What is Web 2.0? Ideas, technologies and implications for education*, research report, JISC Technology and Standard Watch. Available at: <http://21stcenturywalton.pbworks.com/f/What+is+Web+2.0.pdf> (accessed 2 September 2013).
- Ankolekar, A., Burstein, M., Hobbs, J., Lassila, O., Martin, D., McIlraith, S., Narayanan, S., Paolucci, M., Payne, T., Sycara, K., and Zeng, H. (2001), *DAML-S: Semantic Markup for Web Services*, International Semantic Web Working Symposium (SWWS), pp. 39-54. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.29.2967&rep=rep1&type=pdf> (accessed 20 September 2013).
- Bakshi, K. and Karger, D.R. (2005), *End-user application development for the semantic Web*, research paper, ISWC Workshop on the Semantic Desktop - Next Generation Information Management and Collaboration Infrastructure, pp. 123–137.
- Benjamins, R. and Contreras, J. (2002), *Six Challenges for the Semantic Web*, white paper, Intelligent Software Components, Intelligent Software for the Networked Economy (isoco), April. Available at: <http://oa.upm.es/5668/1/Workshop06.KRR2002.pdf> (accessed 2 October 2013).
- Bergman, M. (2001), *The Deep Web: Surfacing Hidden Value*, white paper, The Journal of Electronic Publishing, August. Available at: <http://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.0007.104> (accessed 4 September 2013).
- Berners-Lee, T., Hendler, J. and Lassila, O (2001), *The Semantic Web [Preview]*, Scientific America. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=539724 (accessed 12 September 2013).
- Berners-Lee, T (1998), *Why RDF model is different from the XML model*, World Wide Web Consortium. Available at: <http://www.w3.org/DesignIssues/RDF-XML.html> (accessed 12 September 2013).
- Berners-Lee, T. (1996), *WWW: past, present, and future*, Computer, Vol. 29 No.10, pp. 69-77. Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=539724&tag=1> (accessed 2 September 2013).

Boshoff, W. (2012), *Business imperatives*. Masters in Accounting (Computer Auditing) lecture slides. Stellenbosch University.

Brynjolfsson, E. and Hitt, L.M. (2000), *Beyond Computation: Information technology, Organizational Transformation and Business Performance*, Journal of Economic Perspectives, Vol. 14 No. 4, pp. 23-48.

Bürger, T. (2008), *Towards increased reuse: Exploiting social and content related features of multimedia content on the semantic Web*, International Workshop on Interacting with Multimedia Content in the Social Semantic Web (IMC-SSW'08). Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.143.1454&rep=rep1&type=pdf> (accessed 18 September 2013).

Carabelli, C. (n.d.), *The Definition of "Business Imperative"*, Demand Media. Available at: <http://smallbusiness.chron.com/definition-business-imperative-25055.html> (accessed 9 September 2013).

Campbell, P. L. (2005), *ACobiT Primer*, Sandia National Laboratories, No. SAND2005-3455. Available at: <http://prod.sandia.gov/techlib/access-control.cgi/2005/053455.pdf> (accessed 10 September 2013).

Chiang, H. and Tsaur, W. (2010), *Mobile Malware Behavioral Analysis and Preventive Strategy Using Ontology*, IEEE International Conference on Social Computing/IEEE International Conference on Privacy, Security, Risk and Trust, pp. 1080-1085. Available at: http://www.lasr.cs.ucla.edu/classes/239_1.fall10/papers/ontology.pdf (accessed 7 October 2013).

Clearswift (2007), *Demystifying Web 2.0*, white paper, Clearswift Limited, July. Available at: <http://resources.clearswift.com/ExternalContent/C12CUST/Clearswift/9514/200707> (accessed 28 August 2013).

Cormode, G. and Krishnamurthy, B. (2008), *Key differences between Web 1.0 and Web 2.0*, First Monday, Vol. 13 No. 6. Available at: <http://firstmonday.org/ojs/index.php/fm/article/view/2125/1972> (accessed 29 August 2013).

Davies, J., Fensel, D. and van Harmelen, F. (2002), *Towards the Semantic Web: Ontology-Driven Knowledge Management*, John Wiley, Chichester. Available at: [http://www.iwayan.info/Research/Book/SemWeb/Tmp_Towards%20The%20Semantic%20Web%20-%20Ontology-driven%20Knowledge%20Management%20\(2003\).pdf](http://www.iwayan.info/Research/Book/SemWeb/Tmp_Towards%20The%20Semantic%20Web%20-%20Ontology-driven%20Knowledge%20Management%20(2003).pdf) (accessed 18 September 2013).

Dawson, R. (2007), *Web 2.0 framework*, [blog]. Available at: www.rossdawsonblog.com/Web2 (accessed 28 August 2013).

Dawson, R. (2008), *An enterprise 2.0 Governance Framework-looking for input!*, [blog]. Available at: http://rossdawsonblog.com/Weblog/archives/2008/02/an_enterprise_2.html (accessed 28 August 2013).

DCruz, T. (2009), *Difference Between Web 1.0, Web 2.0 and Web 3.0*, Enzine Articles, available at: <http://ezinearticles.com/?Difference-Between-Web-1.0,-Web-2.0-and-Web-3.0&id=2941533> (accessed 19 October 2013).

Decker, S., Melnik, S., van Harmelen, F., Fensel, D., Klein, M., Broekstra, J., Erdmann, M., and Horrocks, I. (2000), *The Semantic Web: The Roles of XML and RDF*, IEEE Internet Computing, Vol. 4, pp. 63-74. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.81.6109&rep=rep1&type=pdf> (accessed 12 September 2013).

developerWorks Interviews. (2006), Tim Berners-Lee, Originator of the Web and Director of the World Wide Web Consortium, talks about where we've come from, and about the challenges and opportunities ahead, August 2006, [Podcast]. Available at: <http://www.ibm.com/developerworks/podcast/dwi/cm-int082206.txt> (accessed 29 august 2013).

Dietzold, S. and Auer, S. (2006), *Access control on RDF triple stores from a semantic wiki perspective*, The Semantic Web Workshop at 3rd European Semantic Web Conference (ESWC). Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.3708&rep=rep1&type=pdf> (accessed 7 October 2013).

Doughty, K. & Grieco, F. (2004), *IT Governance: Pass or Fail?*, Information Systems Control Journal, Vol. 2, 2005. Available at: <http://www.isaca.org/Journal/Past-Issues/2005/Volume-2/Pages/JOnline-IT-Governance-Pass-or-Fail.aspx> (accessed 8 September 2013).

Eyharabide, V. and Amandi, A. (2012), *Ontology-based user profile learning*, Applied Intelligence, Vol. 36 No. 4, pp. 857-869. Available at: <http://dl.acm.org/citation.cfm?id=2011270> (accessed 7 October 2013).

Eckerson, W. (1999), *BI vs. Knowledge Management*, Information Management. Available at: <http://www.information-management.com/issues/19990201/177-1.html> (accessed 21 September 2013).

Edvardsson, I.R. and Durst, S. (2012), *Knowledge management in SMEs: a literature review*, Journal of Knowledge Management, Vol. 16 No. 6, pp. 879-903. Available at: <http://www.emeraldinsight.com/journals.htm?articleid=17062891> (accessed 21 September 2013).

Evans, D. (2011), *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, white paper, Cisco Internet Business Solutions Group (IBSG), April. Available at: http://www.cisco.com/Web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (accessed 16 May 2013).

- Farah, J. (2012), *Predicting the Intelligence of Web 3.0 Search Engines*, International Journal of Computer Theory and Engineering, Vol. 4 No. 3, pp. 443-445. Available at: <http://www.ijcte.org/papers/503-G1326.pdf> (accessed 04 September 2013).
- Farkas, C. and Huhns, M.N., *Making Agents Secure on the Semantic Web*, IEEE Internet Computing, Vol. 6 No. 6, pp. 76-79. Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1067741> (accessed 2 October 2013).
- Finin, T., Joshi, A., Kagal, L., Niu, J., Sandhu, R., Winsborough, W. and Thuraisingham, B. (2008), *Rowlbac: Role based access control in OWL*, ACM Symposium on Access Control Models and Technologies (SACMAT). Available at: http://ebiquity.umbc.edu/file_directory/papers/391.pdf (accessed 7 October 2013).
- Foley, S.N. and Fitzgerald, W.M. (2008), *Semantic Web and Firewall Alignment*, First International Workshop on Secure Semantic Web (SSW'08). Available at: <http://www.cs.ucc.ie/~simon/pubs/ssw08.pdf> (accessed 7 October 2013).
- García-Crespoa, A., Gómez-Berbísa, J.M., Colomo-Palacios, R. and Alor-Hernández, G. (2011), *SecurOntology: A semantic Web access control framework*, Computer Standards & Interfaces, Vol. 33 No. 1, pp. 42-49. Available at: <http://www.sciencedirect.com/science/article/pii/S0920548909000798> (accessed 7 October 2013).
- Gertz, M., Guldentops, E. and Strous, L.A.M.(2002), *Integrity, Internal Control and Security in Information Systems: Connecting Governance and Technology*, Springer.
- Getting, B. (2007), Basic Definitions: Web 1.0, Web. 2.0, Web 3.0. Available at: www.practicalecommerce.com/articles/464/Basic-Definitions:-Web-1.0,-Web-2.0,-Web-3.0/ (accessed 19 August 2013).
- Ghaleb, F., Daoud, S., Hasna, A., ALJa'am, J.M., El-Seoud, S.A. and El-Sofany, H. (2006), *E-Learning Model Based On Semantic Web Technology*, International Journal of Computing & Information Sciences, Vol. 4 No. 2, pp. 63-71. Available at: <http://www.ijcis.info/Vol4N2/pp63-71.pdf> (accessed 21 September 2013).
- Giannakos, N., and Lapatas, V. (2010), *Towards Web 3.0 Concept For Collaborative e-Learning*, research report, International Multi-Conference on Innovative Developments in ICT. Available at: http://www.academia.edu/417958/Towards_Web_3.0_Concept_for_Collaborative_e-Learning (accessed 4 September 2013).
- Giereth, M. (2005), *On Partial Encryption of RDF-Graphs*, The Semantic Web – ISWC 2005 Lecture Notes in Computer Science, Vol. 3729, pp. 308-322.

- Gil, Y. and Artz, D. (2007), *Towards Content Trust of Web Resources*, Journal of Web Semantics: Science, Services and Agents on the World Wide Web, December. Available at: <http://www.isi.edu/~gil/papers/gil-artz-jws07.pdf> (accessed 2 October 2013).
- Gilbert, D. (1997), *Intelligent Agents: The right Information at the Right Time*, white paper, IBM Corporation, May. Available at: <https://fmfi-uk.hq.sk/Informatika/Uvod%20Do%20Umelej%20Inteligencie/clanky/ibm-iagt.pdf> (accessed 15 September 2013).
- Gilbert, M.R., Abrams, C., Linden, A., Mogull, R., Orans, L. and Wald, B. (2001), *Emerging Technologies for Managing Content*, research report, Gartner, 28 September. Available at: <http://my.gartner.com/portal/server.pt?open=512&objID=260&mode=2&PageID=3460702&resId=341672&ref=QuickSearch&stkw=Guaranteed+e-delivery> (accessed 7 October 2013).
- Golbreich, C., and Wallace, E.K. (2012), *OWL 2 Web Ontology Language: New Features and Rationale (Second Edition)*, World Wide Web Consortium. Available at: <http://www.w3.org/TR/owl2-new-features/> (accessed 7 October 2013).
- Goosen, R. (2012), *The development of an integrated framework in order to implement information technology governance principles at a strategic and operational level for medium- to large-sized South African businesses*. Unpublished masters dissertation, Stellenbosch: Stellenbosch University.
- Grossman, J. (2007), *Seven Business Logic Flaws That Put Your Website At Risk*, white paper, WhiteHat Security, October. Available at: https://www.whitehatsec.com/assets/WP_bizlogic092407.pdf (accessed 28 August 2013).
- Guess, A. (2013), *The Big BI Problems Created by Big Data*, SemanticWeb. Available at: http://semanticWeb.com/the-big-bi-problems-created-by-big-data_b36171#more-36171 (accessed 18 September 2013).
- Halfond, W.G., Viegas, J. and Orso, A. (2006), *A Classification of SQL-Injection Attacks and Counter Measures*, The International Symposium on Secure Software Engineering, March. Available at: <http://www.cc.gatech.edu/fac/Alex.Orso/papers/halfond.viegas.orso.ISSSE06.pdf> (accessed 7 October 2013).
- Hall, B., Khan, B. (2002), *Adoption of new technology*, D.C. Jones (Ed.), New Economy Handbook, Elsevier Science, pp. 230–251. Available at: <http://emlab.berkeley.edu/~bhhall/papers/HallKhan03%20diffusion.pdf> (accessed 15 October 2013).
- Hameed, I. (2004), *Knowledge management and business intelligence: what are the differences*, OnlineBusiness. Available at: <http://onlinebusiness.about.com/> (accessed 18 September 2013).

- Hasnain, A., Al-Bakri, M., Costabello, L., Cong, Z., Davis, I. and Heath, T. (2012), *Spamming in Linked Data*, Third International Workshop on Consuming Linked Data (COLD2012). Available at: http://ceur-ws.org/Vol-905/HasnainEtAl_COLD2012.pdf (accessed 28 September 2013).
- Hayati, P., Potdar, V., Talevski, A., Firoozeh, N., Sarenche, S. and Yeganeh, E. A. (2010), *Definition of spam 2.0: New spamming boom*, 4th IEEE International Conference on Digital Ecosystems and Technologies, pp. 580-584. Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5610590&tag=1> (accessed 28 September 2013).
- Herschel, R.T., Jones, N.E. (2005), *Knowledge management and business intelligence: the importance of integration*, Journal of Knowledge Management, Vol.9 No.4, pp. 45-55. Available at: <http://www.emeraldinsight.com/journals.htm?articleid=1509670> (accessed 18 September 2013).
- Hess, A., and Kushmerick, N. (2003), *Automatically attaching semantic metadata to Web services*, 2nd International Semantic Web Conference (ISWC 2003). Available at: <http://www.isi.edu/info-agents/workshops/ijcai03/papers/hess-ijcai03-iiw1.pdf> (accessed 20 September 2013).
- Horacio, S., Funk, A., Maynard, D. and Bontcheva, K. (2007), *Ontology-Based Information Extraction for Business Intelligence*, *The Semantic Web Lecturer: Notes in Computer Science*, Vol. 4825, pp. 843-856.
- Horrocks, I. (2004), *OWL Rules, OK?*, World Wide Web Consortium. Available at: <http://www.w3.org/2004/12/rules-ws/paper/42/> (accessed 12 September 2012).
- Hotchkies, C. (2004), *Blind SQL Injections Automation Techniques*, Black Hat Briefings USA. Available at: <http://www.sachin0631.0fees.net/sqlinjection.pdf> (accessed 2 October 2013).
- Huang, H.D., Lee, C.S., Kao, H.Y., Tsai, Y.L. and Chang, J.G. (2011), *Malware behavioral analysis system: Twman*, IEEE Symposium on Computational Intelligence for Intelligent Agents. Available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5953604> (accessed 7 October 2013).
- Hussain, S. J. and Siddiqui, M. S. (2005), *Quantified Model of COBIT for Corporate IT Governance*, First International Conference on Information and Communication Technologies, Karachi. Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1598575&tag=1> (accessed 10 September 2013).
- International Data Corporation (2012), *The Changing Role of the IT Organization and the Impact of Skills*, white paper, International Data Corporation Go-to-Market Services, October. Available at: <http://www.findwhitepapers.com/content23728#> (accessed 20 May 2013).

Internet World Stats (2012), Internet usage statistic. Available at: <http://www.internetworldstats.com/stats.htm> (accessed 19 July 2013).

Intervise (n.d.), *The Semantic Web Information with Knowledge*, white paper, Intervise Consultants Incorporated. Available at: <http://www.semantic-experts.com/galleries/default-file/White%20Paper%20Semantic%20Web.pdf> (accessed 05 September 2013).

ISACA (2012), *COBIT 5 Enabling Processes*, ISACA. Available at: <http://www.isaca.org/COBIT/Documents/COBIT5-Ver2-enabling.pdf> (accessed 28 September 2013).

IT Governance Institute (2007), COBIT 4.1. Available at: <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-4-1.aspx> (accessed 27 August 2013).

IT Governance Institute (2005), *Optimising Value Creation From IT Investments*, IT Governance institute. Available at: <http://www.isaca.org/Knowledge-Center/Research/Documents/optimising-value-creation-from-IT.pdf> (accessed 9 September 2013).

Kagal, L., Paolucci, M., Srinivasan, N., Denker, G., Finin, T. and Sycara, K. (2004), *Authorization and privacy for semantic Web services*, Spring Symposium on Semantic Web Services. Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1333035&tag=1> (accessed 7 October 2013).

Kagal, L., Finin, T. and Joshi, A. (2003), *A Policy Based Approach to Security for the Semantic Web*, 2nd International Semantic Web Conference (ISWC2003), September. Available at: <http://www.csee.umbc.edu/~finin/papers/papers/iswc03b.pdf> (accessed 28 September 2013).

Knublauch, H., Fergerson, R.W., Noy, N.F., and Musen, M.A. (2004), *The Protégé OWL Plugin: An Open Development Environment for Semantic Web Applications*, Lecture Notes in Computer Science, Vol. 3298, pp.229-243.

Koper, R. (2004), *Use of the Semantic Web to Solve Some Basic Problems in Education: Increase Flexible, Distributed Lifelong Learning, Decrease Teacher's Workload*, Journal of Interactive Media in Education, Vol. 6. Available at: <http://jime.open.ac.uk/jime/article/viewArticle/2004-6-koper/188> (accessed 21 September 2013).

Kumar, S., Prajapati, R.K., Singh, M. and De, A. (2010), *Realization of Threats and Countermeasure in Semantic Web Services*, International Journal of Computer Theory and Engineering, Vol. 2 No. 6, pp. 919-924. Available at: <http://www.ijcte.org/papers/264-G796.pdf> (accessed 28 September 2013).

- Lange, D.B. and Oshima, M. (1999), *Seven good reasons for mobile agents*, Communications of the ACM, Vol. 42 No. 3, pp. 88-89. Available at: <http://www.moe-lange.com/danny/docs/7reasons.pdf> (accessed 21 September 2013).
- Lašek, I. and Vojtáš, P. (2011), *Semantic Information Filtering - Beyond Collaborative Filtering*, 4th International Semantic Search Workshop. Available at: <http://km.aifb.kit.edu/ws/semsearch11/11.pdf> (accessed 7 October 2013).
- Lawler, P. and Molluzzo, C. (2010), *A Study of the Perceptions of Students on Privacy and Security on Social Networking Sites (SNS) on the Internet*, Journal of Information Systems Applied Research, Vol. 3 No. 12, pp. 1-18.
- Lee, J. and Whang, K. (2006), *Secure query processing against encrypted XML data using Query-Aware Decryption*, Elsevier, Information Sciences, pp. 1928-1947. Available at: <http://dm.kaist.ac.kr/jaegil/papers/infosci06.pdf> (accessed 7 October 2013).
- Lewis, D.J. (2008), *Intelligent agents and the Semantic Web*, developerWorks. Available at: <http://www.ibm.com/developerworks/library/wa-intelligentage/> (accessed 15 September 2013).
- Lu, S., Dong, M., Fotouhi, F. (2002), *The Semantic Web: Opportunities and challenges for next-generation Web applications*, Information Research, Vol. 7 No. 4. Available at: <http://informationr.net/ir/7-4/paper134.html> (accessed 28 August 2013).
- Lynch, J. (2005), *Identity theft in cyberspace: Crime control methods and their effectiveness in combating phishing attacks*, Berkeley Technology Journal, Vol. 20, pp. 259-300.
- Martin, D., Burstein, M., Hobbs, J., Lassila, O., McDermott, D., McIlraith, S., Narayanan, S., Paolucci, M., Parsia, B., Payne, T., Sirin, E., Srinivasan, N., Sycara, K. (2004), *OWL-S: Semantic Markup for Web Services*, World Wide Web Consortium. Available at: <http://www.w3.org/Submission/OWL-S/> (accessed 21 September 2013).
- McGraw, G. (2008), *Software [In] security: Securing Web 3.0*, InformIT. Available at: <http://www.informit.com/articles/article.aspx?p=1217101> (accessed 28 September 2013).
- Melo, D., Rodrigues, P.I., Nogueira, B.V. (2012), *Work Out the Semantic Web Search: The Cooperative Way*, Advances in Artificial Intelligence, Vol. 2012 Article No. 867831. Available at: <http://www.hindawi.com/journals/aai/2012/867831/> (accessed 18 September 2013).
- Medić, A. and Golubović, A. (2010), *Making secure Semantic Web*, Universal Journal of Computer Science and Engineering Technology, Vol. 1 No. 2, pp. 99-104. Available at: <http://www.unicse.org/publications/2010/november/Making%20secure%20Semantic%20Web.pdf> (accessed 2 October 2013).
- Melton, J. and Eisenberg, A. (2001), *Sql multimedia and application packages (sql/mm)*, SIGMOD Record, Vol. 30 No. 4. Available at: <http://delivery.acm.org/10.1145/610000/604280/p97->

melton.pdf?ip=146.232.41.252&id=604280&acc=ACTIVE%20SERVICE&key=C2716FEBFA981EF194FAE17EEFF9EA9FD4E9E3A22F5A9081&CFID=256988813&CFTOKEN=82882342&acm=1382950300f55d44317d0764a211ffd33048214af9 (12 September 2013).

Mercer, C. (n.d.), *Risks and Benefits of the Semantic Web*, eHow Tech. Available at: http://www.ehow.com/info_12195721_risks-benefits-semantic.html (accessed 2 October 2013).

Middleton, P., Halbert, J. and Coyle, F.P. (n.d.), *Security Impacts on Semantic Technologies in the Coming Decade*, research paper, Dallas University. Available at: http://stko.geog.ucsb.edu/sw2022/sw2022_paper4.pdf (accessed 7 October 2013).

Morris, R.D. (2011), *Web 3.0: Implications for Online Learning*, TechTrends, Vol. 55 No. 1, pp. 42-46. Available at: http://download.springer.com/static/pdf/260/art%253A10.1007%252Fs11528-011-0469-9.pdf?auth66=1382776409_7aa9dbcb343b548f43658d5f1dc6709a&ext=.pdf (accessed 04 September 2013).

Naeve, A., Lytras, M., Nejdl, W., Balacheff, N. and Harding, J. (2006), *Advances of semantic Web for e-learning: Expanding learning frontiers*, British Journal of Education Technology, Vol. 37 No. 3, pp.321-330. Available at: <http://www.noe-kaleidoscope.org/public/pub/news/0505/CFP-BJET-SW-for-EL.pdf> (accessed 21 September 2013).

Nematzadeh, A., Pournajaf, L. (2008), *Privacy Concerns of Semantic Web*, Fifth International Conference on Information Technology: New Generation, .pp.1272-1273. Available at: http://www.mathcs.emory.edu/~lpourna/papers/2008_itng.pdf (accessed 28 September 2013).

Noy, N.F., Sintek, M., Decker, S., Crubézy, M., Fergerson, R.W., and Musen, M. (2001), *Creating Semantic Web contents with Protege-2000*, IEEE Intelligent Systems, Vol. 16 No. 2, pp. 60-71. Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=920601&tag=1> (accessed 5 September 2013).

Optify (2103), *How to sell your agency's inbound marketing services*, white paper, Optify. Available at: http://www.optify.net/wp-content/uploads/2012/11/Optify_how_to_sell_your_agencys_inbound_marketing_services.pdf (accessed 21 September 2013).

Orduña, P., Almeida, A., Aguilera, U., Laiseca, X., López-de-Ipiña, D. and Goiri, A.G. (2010), *Identifying Security Issues in the Semantic Web: Injection Attacks in the Semantic Query Language*, research paper, DeustoTech. Available at: <http://www.morelab.deusto.es/publications/2010/orduna2010identifying.pdf> (accessed 2 October 2013).

O'Reilly, T. (2009), *What is Web 2.0*, California: O'Reilly Media Incorporated. Available at: http://books.google.co.za/books?hl=en&lr=&id=NpEk_WFCMdIC&oi=fnd&pg=PT1&dq=defining+Web+1.0&ots=OXSF8jzH-&sig=t6ZW8qlOh1q6Nbve1LA7f6VbVok#v=onepage&q=defining%20Web%201.0&f=false (accessed: 28 August 2013).

O'Reilly, T. (2007), *What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*, Communications & Strategies, No. 1, p. 17, First Quarter 2007. Available at: <http://ssrn.com/abstract=1008839> (accessed 29 august 2013).

Oracle (2011), *Five Key Benefits of Knowledge Management in Customer Service*, white paper, Oracle, October. Available at: <http://www.oracle.com/us/products/applications/5-befit-knowlg-manag-cust-serv-wp-521298.pdf> (accessed 21 September 2013).

Prescott, B. (2012), *Business Sense: Inbound marketing*, Times Standard. Available at: http://www.times-standard.com/business/ci_19898286 (accessed 21 September 2013).

PricewaterhouseCoopers (2013), *Chapter 5: The governance of information technology*, PricewaterhouseCoopers. Available at: <http://www.pwc.co.za/en/king3/the-governance-of-information-technology/index.jhtml> (accessed 8 September 2013).

PricewaterhouseCoopers (2009), *King's Council Understanding and unlocking the benefits of sound corporate governance*, PricewaterhouseCoopers. Available at: http://c.ymcdn.com/sites/www.iodsa.co.za/resource/collection/dd8b591e-3d00-48d5-b2e9-663fedcff131/Benefits_of_sound_corporate_governance.pdf?hhSearchTerms=King+and+Report+and+on+and+corporate+and+governance+and+for+and+South+and+Afri (accessed 5 September 2013).

Quilitz, B., and Leser, U (2008), *Querying distributed RDF data sources with SPARQL*, Proceedings of the 5th European Semantic Web Conference, ESWC 2008, Tenerife, Canary Islands, Spain. Available at: <http://dl.acm.org/citation.cfm?id=1789443&CFID=256988813&CFTOKEN=82882342> (accessed 12 September 2013).

RAF Technology (2004), *Advanced Data Capture Solutions*, white paper, RAF Technology, December. Available at: <http://www.raf.com/download/Semantic%20Search%20Technical%20Whitepaper.pdf> (accessed 18 September 2013).

Rouse, M. (2005), *SOAP (Simple Object Access Protocol)*, SearchSOA. Available at: <http://searchsoa.techtarget.com/definition/SOAP> (accessed 29 September 2013).

Rudman, R. (2013), *Does Knowing the Risk Impact on Web 2.0 Usage and Security Practices of Online Users?* The International Conference on Information Communication Technologies in Education, pp. 395-406. Available at: <http://www.icicte.org/Proceedings2013/Papers%202013/11-2-Rudman.pdf> (accessed 15 October 2013).

Rudman, R.J. (2010), *Incremental risks in Web 2.0 applications*, The Electronic Library, Vol. 28 No. 2, pp. 210-230. Available at:

<http://www.emeraldinsight.com/journals.htm?articleid=1853058> (accessed 28 July 2013).

Rudman, R.J. (2008), *IT governance: a new era*, Accountancy SA, March 2008, pp. 12-14.

Sahibudin, S., Sharifi, M. and Masarat, A. (2008), *Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations*, Second Asia International Conference on Modeling & Simulation. Available at:

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4530569> (accessed 2 September 2013).

Sampson, D. G., Lytras, M. D., Wagner, G. & Diaz, P (2004), *Ontologies and the Semantic Web for E-learning*, The Journal for Educational Technology & Society, Vol. 7 No. 4, pp. 26-28. Available at:

http://www.ebiblioteka.lt/resursai/Uzsienio%20leidiniai/IEEE/English/2006/Volume%207/Issue%204/Jets_v7i4.pdf#page=87 (accessed 21 September 2013).

Shabajee, P. (2006), *Informed consent on the semantic Web – issues for interaction and interface designers*, The Third International Semantic Web User Interaction Workshop (SWUI), Fifth International Semantic Web Conference (ISWC). Available at:

<http://swui.semanticWeb.org/swui06/papers/Shabajee/Shabajee.pdf> (accessed 11 October 2013).

Shaikh, F., Siddiqui, U.A., Shahzadi, I., Jami, S.I., and Shaikh, Z.A. (2010), *SWISE: Semantic Web based intelligent search engine*, International Conference on Information and Emerging Technologies (ICIET). Available at:

<http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05625670> (accessed 21 September 2013).

Shapovalenko, D. (2008), *Mini research: Semantic Web*, [blog]. Available at:

http://shapovalenko.typepad.com/denis_shapovalenko/2008/03/mini-research-s.html (accessed 29 October 2013).

Sheth, A. and Meersman, R. (2002), *Amicalola Report: Database and Information Systems Research Challenges and Opportunities in Semantic Web and Enterprises*, ACM SIGMOD Record, Vol. 31 No. 4, pp. 98-106. Available at:

http://www.sigmod.org/publications/sigmod-record/0212/R1.Amicalola_Final_Report.pdf (accessed 17 September 2013).

South Africa (2009), *Privacy and Data Protection Report*, Pretoria: Department of Justice. Available at:

http://www.justice.gov.za/salrc/reports/r_prj124_privacy%20and%20data%20protection2009.pdf (accessed 6 September 2013).

Sowa, J.F. (2009), *Building, Sharing, and Merging Ontologies*. Available at:

<http://www.jfsowa.com/ontology/ontoshar.htm> (accessed 12 September 2013).

- Spencer, T. (2009), *The Implications of Web 3.0 on the Strategy and Vision of Businesses*, Travis Spencer, [blog], 21 February 2009. Available at: <http://travisspencer.com/blog/2009/02/the-implications-of-Web-30-on.html> (accessed 20 May 2013).
- Stoneburner, G., Goguen, A., and Feringa, A. (2002), *Risk management guide for information technology systems: Recommendations of the national institute of standards and technology*, National Institute of Standards and Technology (NIST), Special Publication 800-30. Available at: <http://www.security-science.com/pdf/risk-management-guide-for-information-technology-systems.pdf> (accessed 6 September 2013).
- Su, Z. and Wassermann, G. (2006), *The essence of command injection attacks in Web applications*, ACM Symposium on Principles of Programming Languages (POPL). Available at: <http://www.cs.ucdavis.edu/~su/publications/popl06.pdf> (accessed 2 October 2013).
- Sylvester, A., Tate, M. and Johnstone, D. (2011). *Beyond synthesis: re-presenting heterogeneous research literature*, Behaviour & Information Technology. Available at: http://www.tandfonline.com/doi/abs/10.1080/0144929X.2011.624633#.UmZQO3B_PQh (accessed 19 July 2013).
- Tarrant, D., Hitchcock, S., and Carr, L. (2011), *Where the Semantic Web and Web 2.0 Meet Format Risk Management: P2 Registry*, The International Journal of Digital Curation, Vol. 6 No. 1, pp. 165-181. Available at: <http://www.ijdc.net/index.php/ijdc/article/view/171/239> (accessed 04 September 2013).
- TechTerms (2013). Available at: <http://www.techterms.com/list/r> (accessed 5 September 2013).
- The Economist Intelligent Unit (2013), *An expanding network of risk and opportunity: How UK SMEs are under-estimating the growing complexity of technology*, white paper, Zurich, May. Available at: <http://www.managementthinking.eiu.com/sites/default/files/downloads/An%20expanding%20Onetwork%20of%20risk%20and%20opportunity.pdf> (accessed 24 July 2013).
- The National Computing Centre (2005), *IT Governance Developing a successful governance strategy*, white paper, The National Computing Centre. Available at: <http://www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Prepare-for-the-Exam/Study-Materials/Documents/Developing-a-Successful-Governance-Strategy.pdf> (accessed 25 October 2013).
- Thomson, L.M. (2009), *What is corporate governance?* The Economic Times. Available at: http://articles.economictimes.indiatimes.com/2009-01-18/news/28462497_1_corporate-governance-satyam-books-fraud-by-satyam-founder (accessed 5 September 2013).
- Vaculin, A. and Sycara, K. (2007), *Specifying and Monitoring Composite Events for Semantic Web Services*, Fifth European Conference on Web Services, pp.87-96. Available at: <http://www.vaculin.com/downloads/vaculin-ecows07-MonitoringCompositeEvents.pdf> (accessed 7 October 2013).

Van Grembergen, W., and De Haes, S. (2008), *Implementing Information Technology Governance: Models, Practices and Cases*, IGI Global, pp. 1-270.

Verizon (n.d.), *Web 3.0: Its Promise and Implications for Consumers and Business*, white paper, Verizon Business. Available at: http://www.verizonenterprise.com/resources/whitepapers/wp_Web-3-0-promise-and-implications_a4_en_xg.pdf (accessed 2 May 2013).

Villata, S., Delaforge, N., Gandon, F. and Gyrard, A. (2011), *Social semantic Web access control*, 4th International Workshop Social Data on the Web (SDoW2011). Available at: http://sdow.semanticWeb.org/2011/pub/sdow2011_paper_5.pdf (accessed 7 October 2013).

Watson, H.J. and Wixom, B.H. (2007), *The current state of business intelligence*, Computer, Vol. 40 No. 9, pp. 96–99. Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4302625&tag=1> (accessed 18 September 2013).

Webopedia (2013), *OWL*, Webopedia. Available at: http://www.Webopedia.com/TERM/O/Ontology_Web_Language.html (accessed 5 September 2013).

Websense (2009), *Implementing Best Practices for Web 2.0 Security with the Websense Web Security Gateway*, white paper, Websense, June. Available at: https://www.Websense.com/assets/white-papers/Best_Practices_WSG_WEB.PDF (accessed 28 August 2013).

Webschool (2013), *Web Service Tutorial*, Webschool.com. Available at: <http://www.w3schools.com/Webservices/default.asp> (accessed 12 September 2013).

Webster, J. and Watson, R.T. (2002), *Analysing the past to prepare for the future: writing a literature review*, MIS Quarterly, Vol. 26 No. 2, pp. xiii-xxiii.

Weill, P. (2004), *Don't Just Lead, Govern: How Top-Performing Firms Govern*, MIS Quarterly Executive, Vol. 3 No. 1, pp.1-17. Available at: <http://www.umsl.edu/~lacitym/topperform.pdf> (accessed 8 September 2013).

Whittaker, C., Ryner, B. and Nazif, M. (2010), *Large-Scale Automatic Classification of Phishing Pages*, The Network and Distributed System Security Symposium (NDSS). Available at: <http://www.australianscience.com.au/research/google/35580.pdf> (accessed 2 October 2013).

Wikipedia (2013a), *Inbound marketing*, Wikipedia. Available at: http://en.wikipedia.org/wiki/Inbound_marketing (accessed 21 September 2013).

Wikipedia (2013b), *RDF Schema*, Wikipedia. Available at: http://en.wikipedia.org/wiki/RDF_Schema (accessed 5 September 2013).

Wikipedia (2013c), *SPARQL*, Wikipedia. Available at: <http://en.wikipedia.org/wiki/SPARQL> (accessed 5 September 2013).

Wikipedia (2013d), *Uniform resource identifier*, Wikipedia. Available at: http://en.wikipedia.org/wiki/Uniform_resource_identifier (accessed 12 September 2013).

Wolfram, C. (2010) Interviewed by Nicole Kobie on *Communicating with Apps in Web 3.0*, IT Pro, 17 March. Available at: <http://www.itpro.co.uk/621535/qa-conrad-wolfram-on-communicating-with-apps-in-Web-30> (accessed 04 September 2013).

Youn, S. and McLeod, D. (2007), *Efficient spam email filtering using adaptive ontology*, International Conference on Information Technology, pp. 249-254. Available at: <http://www.academypublisher.com/jsw/vol02/no03/jsw02034355.pdf> (accessed 7 October 2013).

Zhong, N. (2003), *Toward Web Intelligence*, Advances in Web Intelligence: Lecture Notes in Computer Science, Vol. 2663, pp. 1-14.

APPENDICES

Appendix 1: Control framework COBIT 5 control processes identified that can be implemented to mitigate risks associated with Web 3.0 technologies

All the COBIT 5 control processes were taken into account during the identification of control procedures and risks associated with the control processes. Only the key processes were listed in the table below.

Control process as defined in control framework COBIT 5	Risks identified	Risk impact with relation to Web 3.0 technologies (High, Medium or Low)	Safeguards to lower risks to an acceptable level
AP001.02 Establishing roles and responsibilities of IT personnel and other parties responsible for creating and implementing effective IT policies. Responsibility and accountability need to be allocated to the authorised parties.	<ul style="list-style-type: none"> • Ineffective policies regarding the use of Web 3.0 technologies. • Policies not reviewed regularly. • Policies not updated on a regular basis to ensure adaption to changing technologies. 	Medium	<ul style="list-style-type: none"> • Allocate responsibility to individual IT personnel by means of job descriptions and definitions. • Regularly review management activities, and follow up on discrepancies.
AP004.03 Monitor the technological environment to identify emerging technologies and its potential to create value. When monitoring new technologies, also identify emerging trends in information security.	<ul style="list-style-type: none"> • Adoption of new technologies without implementing the necessary controls to mitigate the threats these technologies pose. 	Medium	<ul style="list-style-type: none"> • Perform research in order to gain knowledge about trending technologies, and the possible threats associated with them. • Identify new safeguards associated with new technologies.
BAI05.07 Sustain changes through effective training and education of new staff members.	<ul style="list-style-type: none"> • Developers with limited knowledge of new technologies, develop software 	High	<ul style="list-style-type: none"> • Educate users and developers on the risks associated with the use and development of new technologies. • Coordinate learning

With the adoption of new technologies, current staff members also need effective training in the use of these technologies.	and languages that are easily infected by malicious scripts.		campaigns to ensure collaborative learning sessions with annual review sessions. <ul style="list-style-type: none"> Review the educational process, and identify changes in technologies and possible improvements needed.
DSS02.04 Identify the symptoms of possible incidents, determine their possible causes, and decide how these incidents can be resolved.	<ul style="list-style-type: none"> Incidents (risks as identified in section 3.4), occur on system, but are not reported or acknowledged. 	Medium	<ul style="list-style-type: none"> All incidents or symptoms of incidents, should be logged and reported. If there is no current solution for an incident, it should be logged as well, and investigated further.
DSS02.07 Track analysis and incident reports, and review to ensure continual improvement.	<ul style="list-style-type: none"> Incidents (risks as identified in section 3.4), occur on system but are not reported or acknowledged. Incidents are reported but not resolved or prevented by underlying control. 	High	<ul style="list-style-type: none"> A detailed log of all unwanted and harmful actions recorded on the system, should be kept. The report should be reviewed regularly to ensure incidents are resolved promptly. Recurring incidents should be investigated in depth, and underlying controls should be re-evaluated in order to identify the improvement needed.
DSS03.01 Implement procedures to report problems, including problem classification, categorising and prioritisation.	<ul style="list-style-type: none"> Refer DSS02.07 	Medium	<ul style="list-style-type: none"> Refer DSS02.07
DSS05.01 Implement protective, detective and corrective	<ul style="list-style-type: none"> Unauthorised access to sensitive information. 	High	<ul style="list-style-type: none"> Install real time active malicious software tools (ontology driven anti-

<p>measures to safeguard the system against malware.</p> <p>This includes viruses, worms spyware, query language injections and spam.</p>	<ul style="list-style-type: none"> • Unauthorised people performing unauthorised activities. • Parameter manipulation. • Identity theft and social phishing. • Malicious query language injections. • Network eavesdropping and message relay. 		<p>malware programs like TWMAN), which are up to date and are updated - automatically or semi-automatically- when new patches are distributed.</p> <ul style="list-style-type: none"> • Communicate the risk of malware, and ensure that preventative procedures are explained to users. • Ensure that anti-malware software are distributed centrally (version and patch-level), in order for all terminals to be protected by standardised software. • Use spam filtering (like semantic data crawlers), to filter emails, and protect users against unsolicited information. • Review the anti-malware software on a regular basis to identify new threats, or whether upgrades are needed.
<p>DSS05.02 Use measures to ensure all methods of connectivity are secure.</p>	<ul style="list-style-type: none"> • Refer DSS05.01 	High	<ul style="list-style-type: none"> • Implement network filtering methods (semantic data crawlers). • Encrypt data transmitted electronically over networks (XML and RDF encryption). • Implement secure access control (ROWLBAC and S4AC). • Install firewall software to limit intrusion (firewall agents). • Make use of browser and network configuration to secure transmissions. • Test the system by attempting to penetrate it, and review adequacy of system protection.

<p>DSS05.03 Ensure that endpoints (e.g. laptops, desktops, server and other mobile devices and software), are configured securely.</p>	<ul style="list-style-type: none"> • Refer DSS05.01 	<p>High</p>	<ul style="list-style-type: none"> • Configure hardware and operating system in a secure manner. • Encrypt data stored according to priority. • Control access to endpoint devices through remote access control as well as physical protections (e.g. passwords and lock behind closed doors). • When devices become obsolete, dispose of end point devices in a secure manner.
<p>DDS05.04 Ensure that all users have the correct level of access rights, and that the rights allocated to users have been authorised.</p>	<ul style="list-style-type: none"> • Unauthorised access to sensitive information. • Legal actions against organisations due to leakage, or use of sensitive information by unauthorised personnel. 	<p>High</p>	<ul style="list-style-type: none"> • Review if changes to access rights have been documented and approved by authorised person. • Analyse access rights by comparing them with the correlating business function and processing requirements, to ensure that the right level of access have been granted. • Segregate and review all user account privileges on a regular basis. • Ensure that all users and their access rights are uniquely identifiable.
<p>DSS05.07 Monitor and review the infrastructure for security related incidents through the use of intrusion detection tools.</p>	<ul style="list-style-type: none"> • Harmful and unauthorised intrusion identified but not reported, nor controls implemented to control the risk. • Recurring incidents are not properly investigated, and no controls are implemented to stop recurrence. 	<p>High</p>	<ul style="list-style-type: none"> • Keep a log of security related events associated with unusual use of Web 3.0 technologies. • Monitor the potential threats in correlation to the actual recorded threats. • Review the security logs regularly, and consider improved safeguards to mitigate the risks.

